# Réseaux
# Introduction

## Première année

ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

iTii BASSE-NORMANDIE

P Lefebvre - 2023

L'École des INGÉNIEURS Scientifiques

# Organisation

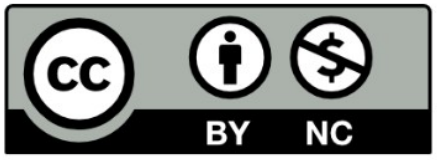
- 1h CM
- 3h TD

# Licence du document

Auteurs

- FOUREY Sébastien
- LEVEE Freddy
- LEFEBVRE Philippe





# Réseaux de télécommunications

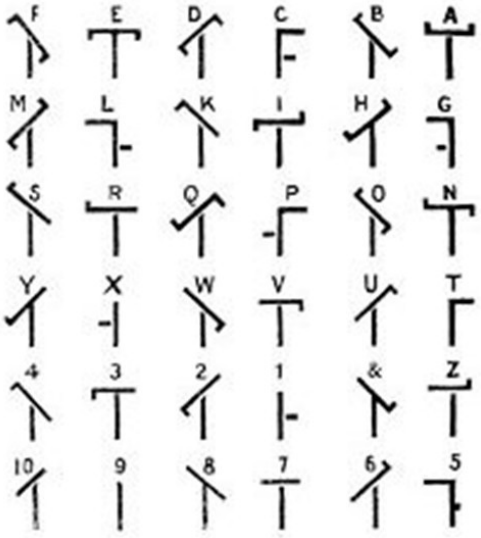
- Le modèle OSI
- Les méthodes d'accès : ethernet, wifi, GSM/GPRS/UMTS, fibre optique, liens série.
- La commutation de paquet / circuits virtuels
- La couche réseau : IP
- La couche transport (UDP, TCP)
- La sécurité

# *Historique*

Muraille de chine, 400 av. JC. : Tour de signaux

Claude Chappe et son télégraphe – 1793 (Paris-Lille),

utilisé jusqu’en 1854 par l’armée.

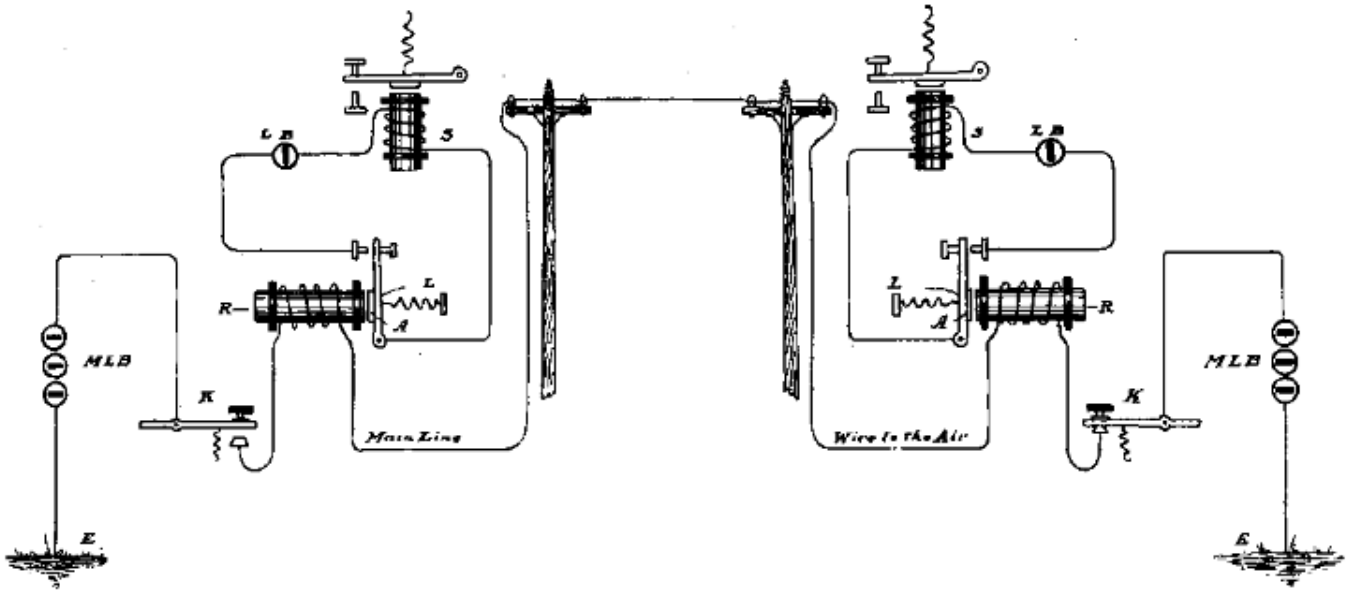



## Télégraphe électrique

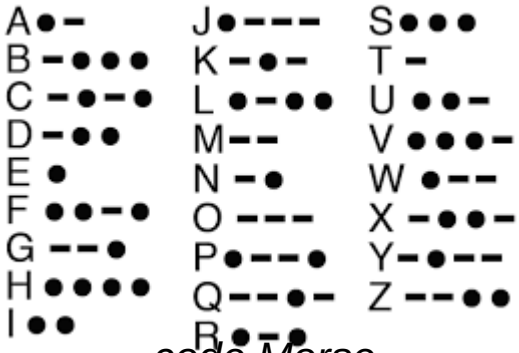
Gauss and Weber, 1833 ( Göttingen Observatory)

Cooke and Wheatstone, 1837 (2 fils,  Great Western Railway )

Samuel Morse, 1844 (1 fil)




The Main Line Circuit.




*code Morse*

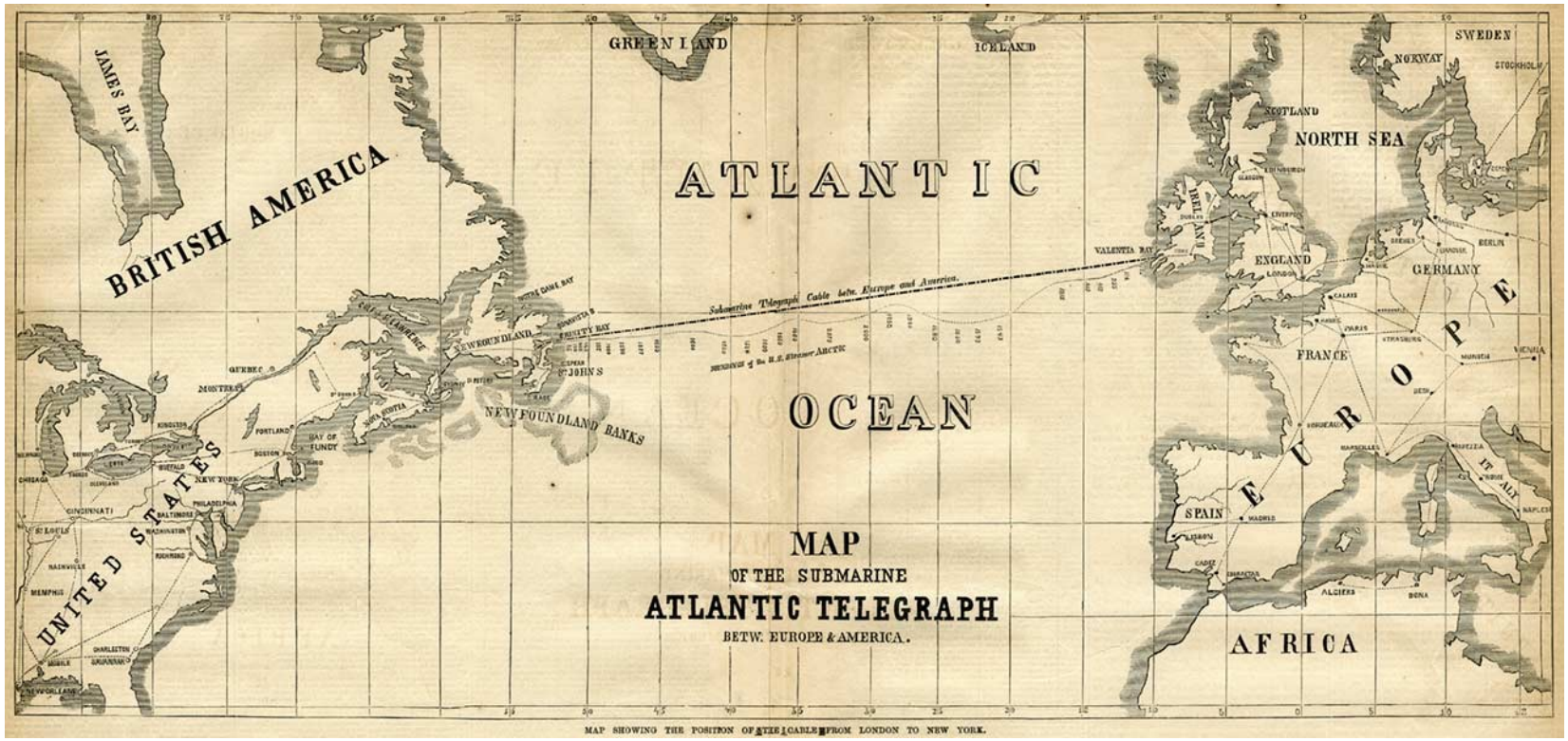
# Historique

Premier câble de télégraphe

opérationnel transatlantique – 1866

sans répéteur

*navire cablier (wikipedia)*



# Historique



Bell et le téléphone - 1870

Graham Bell

*Table de commutation – city of Vancouver (1940)*

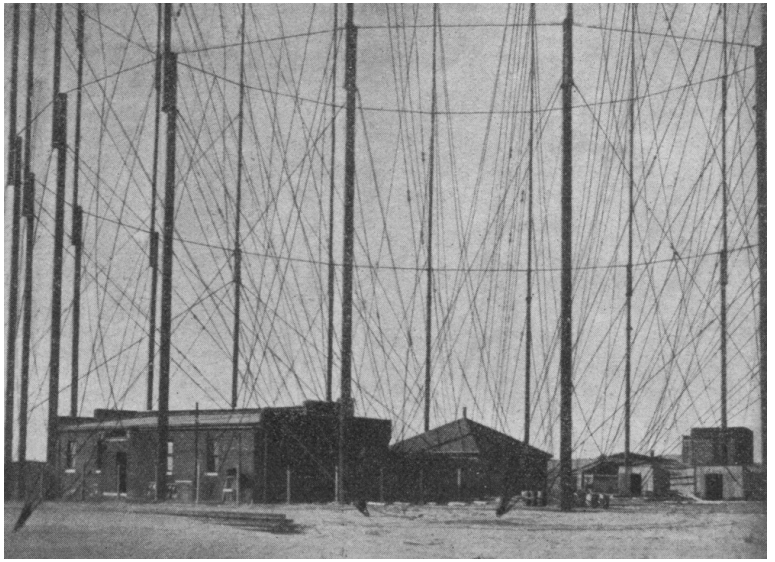
# *Historique*

Dès 1895, Hertz, Popov, Marconi, Tesla font des expérimentations sur les ondes électromagnétiques.

1901, Guglielmo Marconi réalise la première transmission radio transatlantique

1957 Spoutnik

*spoutnik*



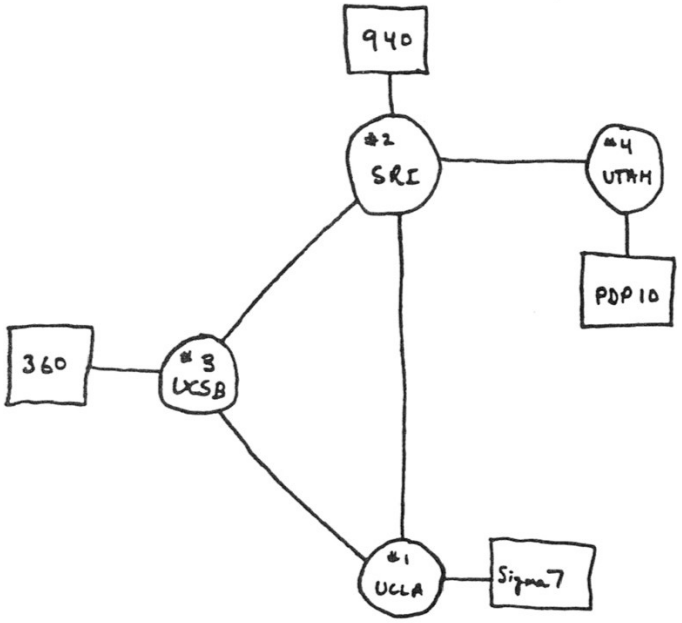
*Antenne TSF en 1901 (wikipedia)*

# Historique



1969, 40 terminaux peuvent dialoguer entre eux : ARPANET, la naissance du réseau Internet.

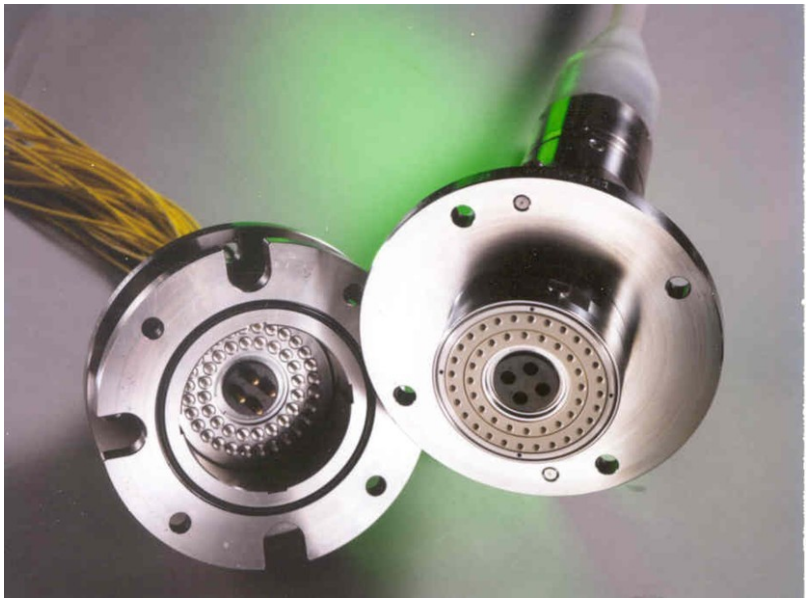
*DEC PDP10 (UTAH)*



# *Historique*

1950, Alfred Kastler invente le laser

1977, premier système de communication par fibre optique installé à Chicago



*connecteur de câble sous-marin (Antares) 48 fibres.*
*Au centre, câbles électriques pour alimentation des répéteurs*

**Record mondial de transmission optique**

**38,4 Tbits/s**

(térabits par seconde, millions de mégabits par secondes)
réalisé sur le réseau fibre opérationnel d'Orange
sur les 762 km de la liaison Lyon-Marseille-Lyon, en 2015

**Record de capacité de transmission à**

**1,5 Tbits/s**

entre Varsovie et Wroclaw
(CP Orange Pologne / Nokia du 21 juillet 2016)

*2016 - record de transmission par fibre optique Orange/Nokia (1,5 Tb/s sur 1 seule fibre de 870 km)*

***2022 – 1,2 Pb/s répartis sur 4 fibres de 52 km (NICCT)***

# *Prévisions (Cisco) faites en 2020 pour 2023*

***2/3 de la population mondial a accès a internet et 70 % a accès a un mobile***

***Le nombre d'appareil connectés est 3x celui de la population mondiale***

***66 % des TV sont connectés en UHD (15 à 18 Mbps)***

Le dernier datacenter de Facebook consomme 100 MW

Une tranche de centrale produit $1{,}3 \times 10^9$ W. La France compte 56 tranches qui produisent 70 % de l'électricité française, et consomme 40 % de l'énergie primaire Française.

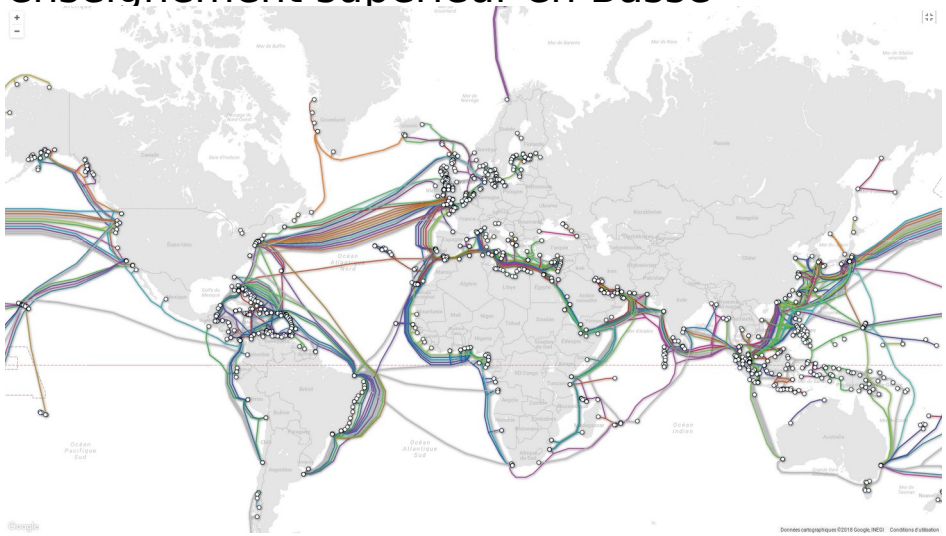
Au total, le numérique consomme 10 à 15 % de l'électricité mondiale, soit l'équivalent de 100 réacteurs nucléaires. **Et cette consommation double tous les 4 ans !**

***Les réseaux sont classés en catégories en fonction de leur grandeur :***

- PAN (Personnal Area Network) : ~ qq m
  - Bluetooth, réseau sans fil entre un téléphone mobile et son oreillette
  - Zigbee réseau de capteurs sans fil (commande de volets...)

- LAN (Local Area Network) : ~ qq  100 m
  - Ethernet pour le réseau d'une entreprise.
  - Wifi

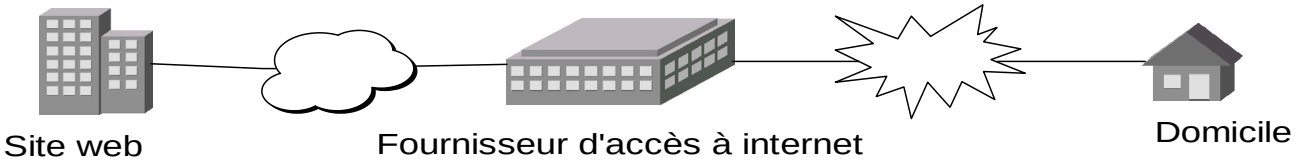
- MAN (Metropolitan Area Network) : qq km
  - Vickman, le réseau d'interconnexion de l'enseignement supérieur en Basse-Normandie.
- WAN ( Wide Area Network ) : le monde
  - comme le réseau Internet, bien sûr...
  - Le réseau téléphonique



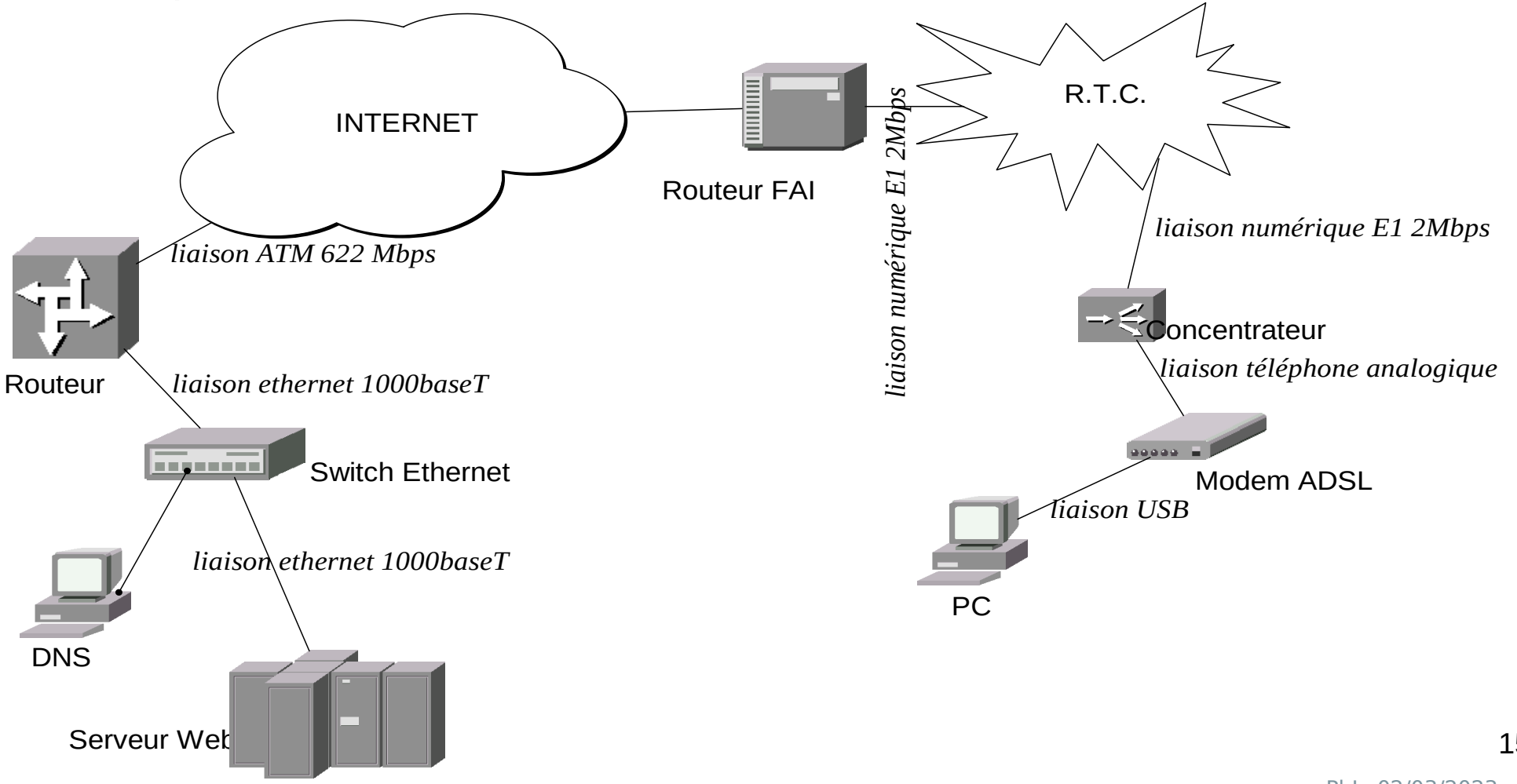
*Quelques débits nécessaires à la réception en temps réel :*

- voix codée en RPE-LTP (GSM) : 13 kbps
- voix non codée (PCM) : 64 kbps (débits des vieux modem)
- HI-FI codée en MPEG3 : 128 kbps
- vidéo au format UltraHD 4K : 25 Mbps

Délai maximum d'acheminement garantissant un bon confort d'interactivité perceptible par l'homme : **50 ms**



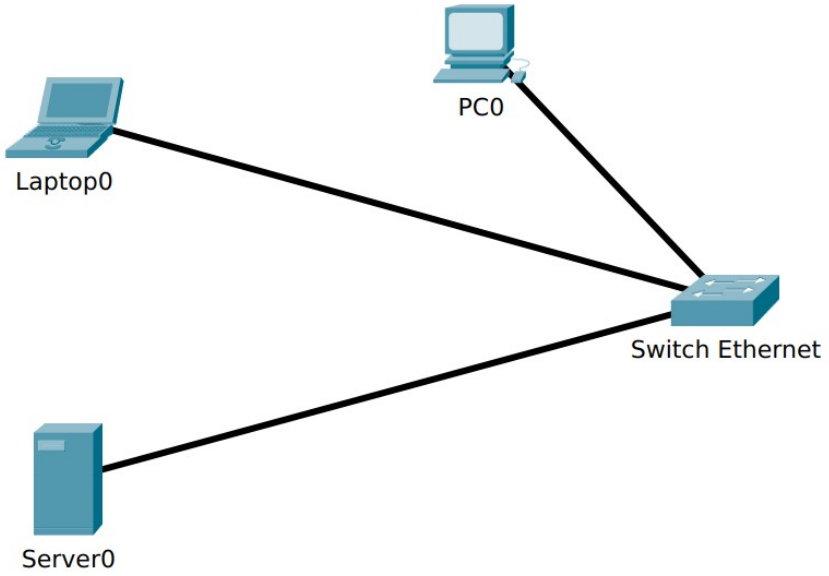

# Un exemple de communication : consultation d'un site web



## Exemple de  problèmes à résoudre : (découpage selon le modèle OSI)

Couche 1 (physique)

- Quels niveaux de tension sur la ligne ?
- Quel codage ?
- Quelle cadence ?
- Quelle forme de connecteur ?



Couche 2 (liaison)

- Comment s'assurer du début d'un envoi d'information ?
- Comment se synchroniser (vitesse des horloges récepteur/émetteur) ?
- Comment être sûr qu'il n'y a pas eu d'erreurs de transmission ?
- L'USB 2.0 émet à 400 Mbps, l'ADSL à 128 kbps. Comment éviter l'engorgement au niveau du modem (contrôle de flux) ?
- Le serveur web et la machine DNS peuvent vouloir parler en même temps. Comment gérer le tour de parole ?
- Comment faire pour envoyer les informations du serveur web au routeur et non au DNS ?
- Puis-je multiplexer mes données sur plusieurs liaisons physiques ?

# Exemple de  problèmes à résoudre (suite) :

## Couche 3 (réseau)

- Comment aller du routeur au routeur du FAI ? Par quel chemin ?
- Je peux joindre tout le monde. Comment gérer l'unicité des adresses ?
- Y a-t-il un centre de tri qui connaît toutes les adresses de tout l'internet ?
- Et si un second message arrive avant un premier, comment les remettre dans l'ordre ?
- Et si mon message pendant son voyage arrive sur un support qui n'accepte que des petits messages ! Comment segmenter ?
- Et si un message ne trouve pas son destinataire ?

## Couche 4 (transport)

- Le message arrive enfin sur ma machine ! Pourquoi est-il acheminé sur mon navigateur et pas sur mon logiciel de peer2peer ?
- Au fait, après avoir traversé autant de supports physiques différents, le message a-t-il été altéré ?
- Comment être sûr que le message soit arrivé ?
- Comment initier et rompre proprement le dialogue ?
- Comment faire patienter le l'émetteur ?

## Exemple de  problèmes à résoudre (suite) :

**Couche 5 (session)**

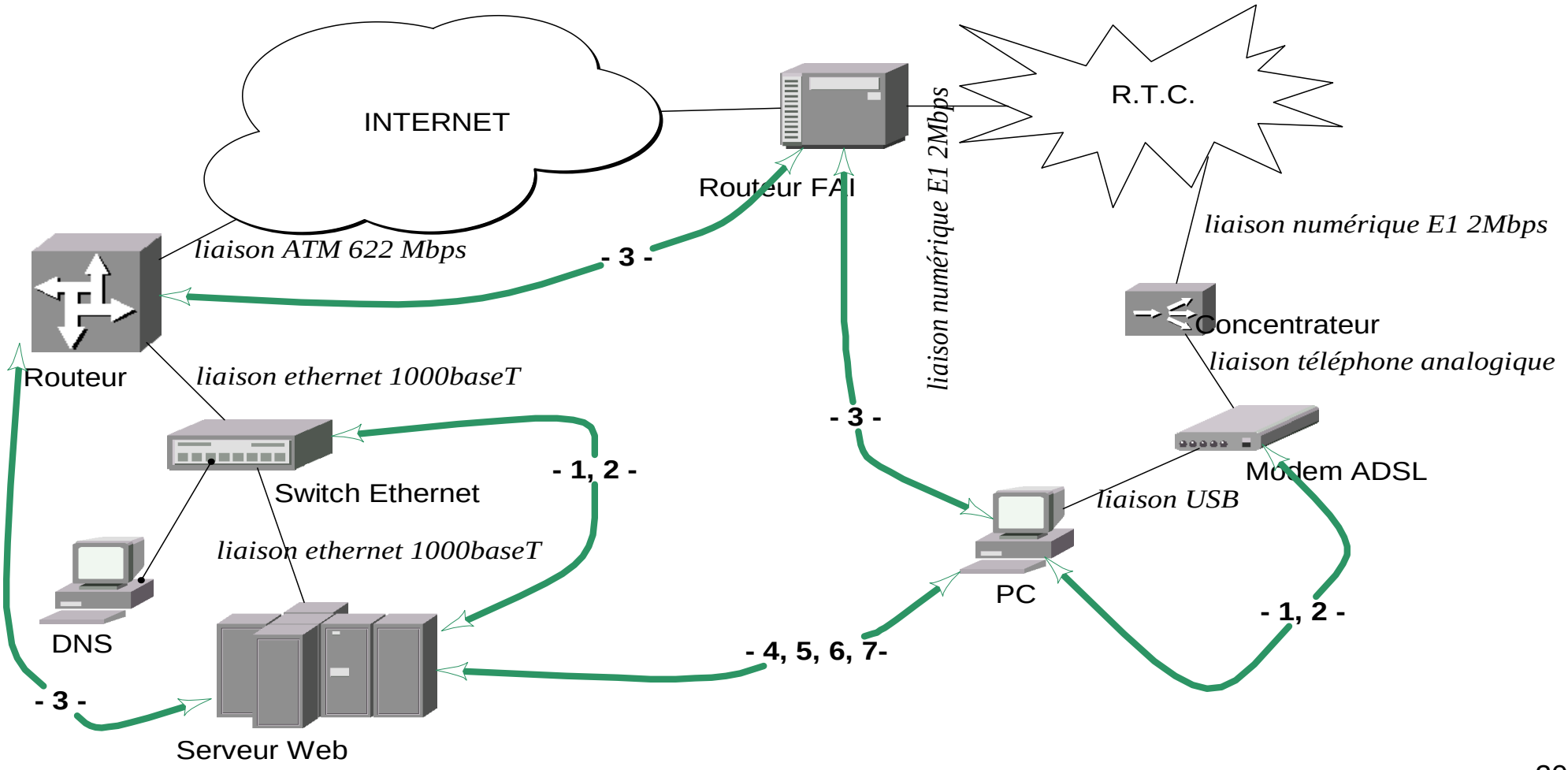
- Comment m'assurer de l'identité de l'utilisateur ?
- Suis-je capable de reprendre correctement une session brutalement interrompue ?

**Couche 6 (présentation)**

- Et si j'envoie le mot «Été »  sera-t-il bien transmis ?
- Et les nombres entiers du destinataire : 16 bits ou 32 bits ?
- Et si je lui envoie une image, quel format ?

**Couche 7 (application)**

- Le courrier électronique, le partage de fichier, la vidéo-conférence, un jeu, un annuaire...


INTERNET
Routeur FAI
R.T.C.
liaison numérique E1 2Mbps
liaison numérique E1 2Mbps
liaison ATM 622 Mbps
- 3 -
Concentrateur
liaison téléphone analogique
Routeur
liaison ethernet 1000baseT
- 3 -
Modem ADSL
Switch Ethernet
- 1, 2 -
liaison USB
liaison ethernet 1000baseT
PC
DNS
- 1, 2 -
- 4, 5, 6, 7-
- 3 -
Serveur Web

# Le modèle OSI de l'ISO

Modèle Open System Interconnection de l'International Standards Organization

Organismes classiques de normalisation:

- International Organization for Standardization (ISO). ex : OSI
- American National Standards Institute (ANSI). ex : FDDI
- Electronic Industries Association (EIA). ex : RS 232C
- Institute of Electrical and Electronic Engineers (IEEE). ex : 802.3
- International Telecommunication Union Telecommunication Standardization Sector (ITU-T). ex : X25
- Internet Activities Board (IAB). ex : RFC, TCP/IP.

Élaboré en 1984 ; idée : **Compatibilité entre tous les systèmes !**

Différents niveaux de communication : bits, octets, trames, fichiers... => modèle en couches.

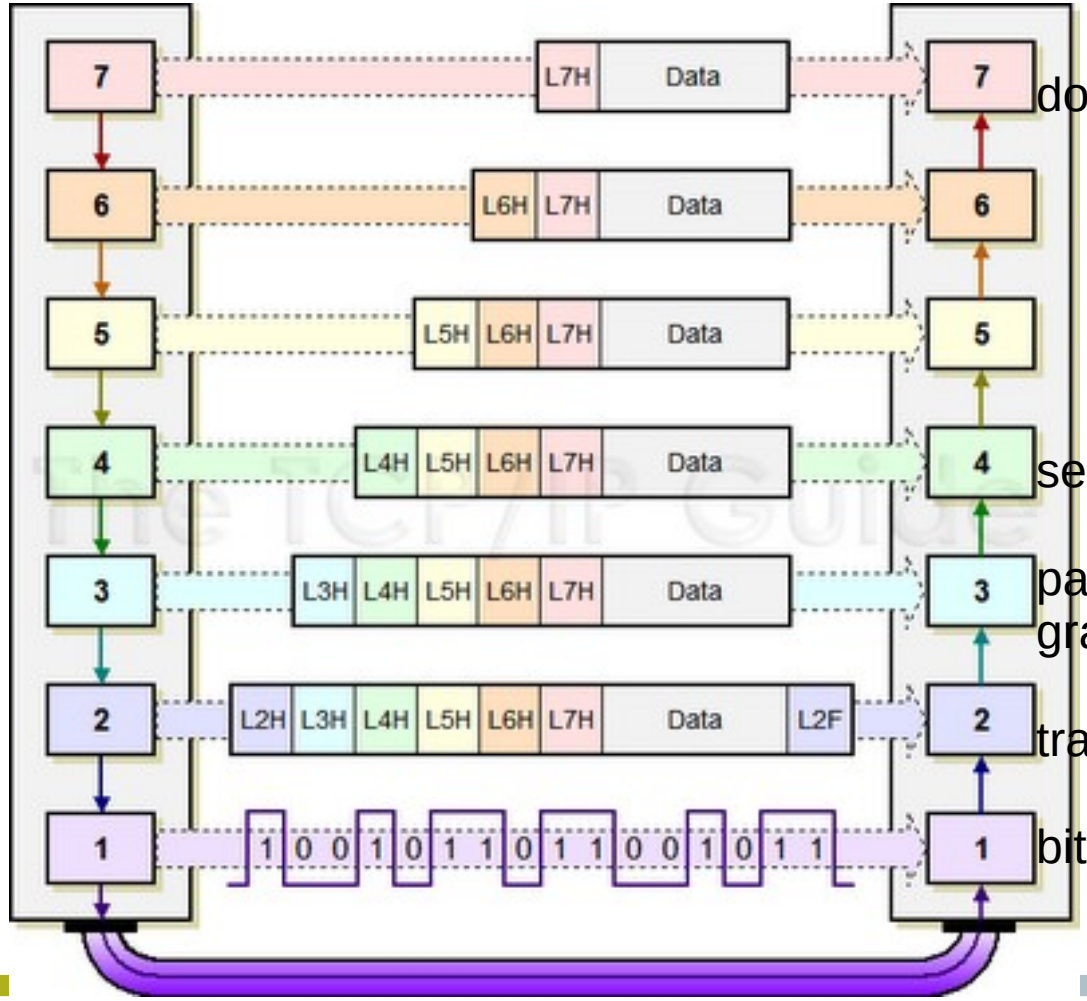
# Le modèle OSI de l'ISO

| No | nom | Rôle | Exemple de PDU | exemple de protocole |
|---|---|---|---|---|
| 7 | Application | Applications s'appuyant sur le réseau : transfert de fichiers, émulation de terminal, messagerie, partage de fichiers, web… | fichier | telnet, HTTP, mail, NFS, FTP |
| 6 | Présen-tation | Conversion des données numériques propres au réseau dans leur version finale ou abstraite compréhensible par le programme. Cette couche est souvent associée à un langage possédant des règles lexicales (les mots), syntaxiques (la grammaire) et sémantique (le sens). | chaîne de caractères | ASN1... |
| 5 | Session | Gestion d'une session : ouverture, mots de passe, reprise en cas d'erreur, fermeture. | | Netbios |
| 4 | Transport | Multiplexage/démultiplexage des paquets, segmentation, contrôle de flux, correction des erreurs. Service de bout en bout. | paquet | ~TCP |
| 3 | Réseau | Service point à point. Assure le routage, l'adressage. | trame | ~IP |
| 2 | Liaison | Délimitation d'une trame, contrôle et correction d'erreurs, contrôle de flux, règle d'accès au médium. Service point à point. | trame | HDLC |
| 1 | Physique | Conversion des signaux électriques en bits. Définition des caractéristiques électriques et mécaniques du support de transmission. | bits | ~ethernet |

# Le modèle OSI de l'ISO

L'information est regroupées coupée en PDU : Protocol data unit. Le nom de la PDU change selon le niveau du modèle.

Encapsulation des PDU : la PDU de couche N est contenue dans la PDU de couche N-1.




PDU

données

segment

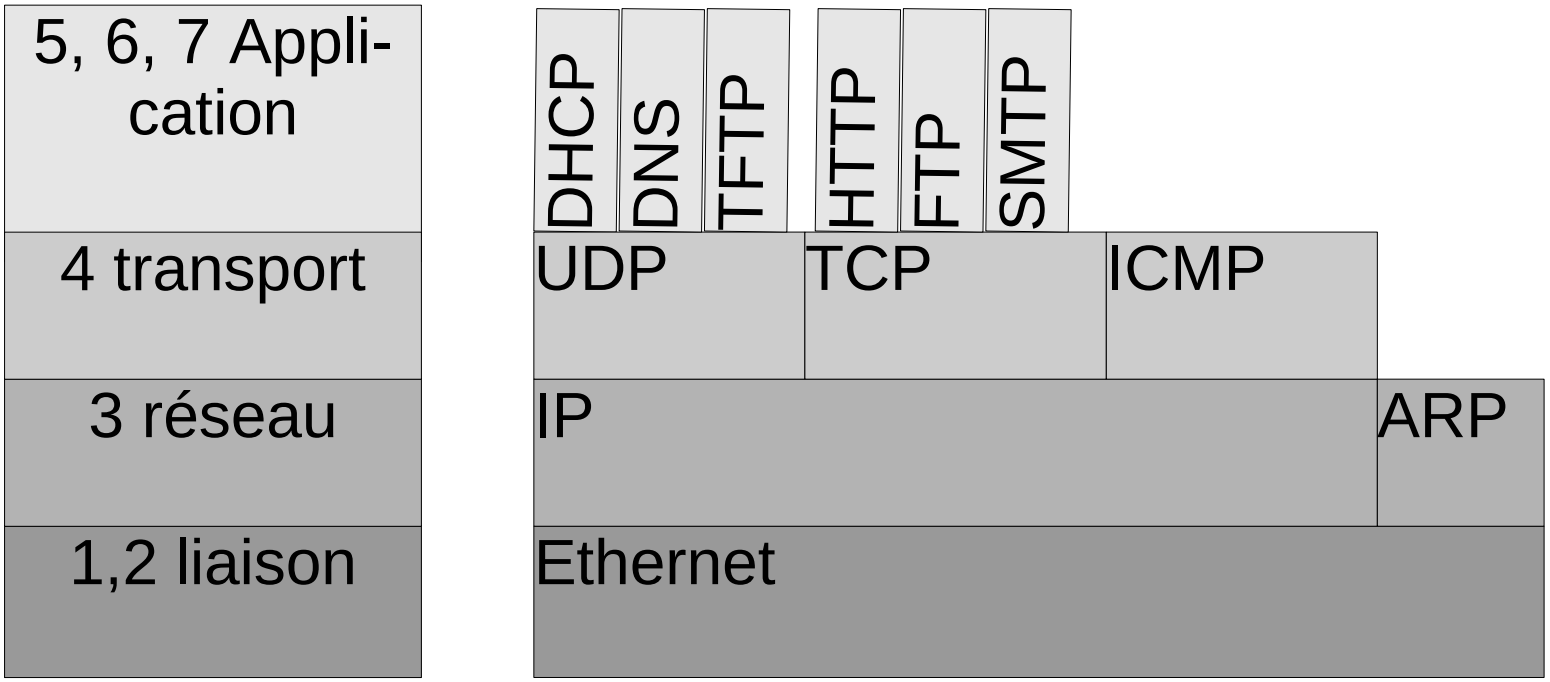
paquet, data-gramme

trame, cellule

bit

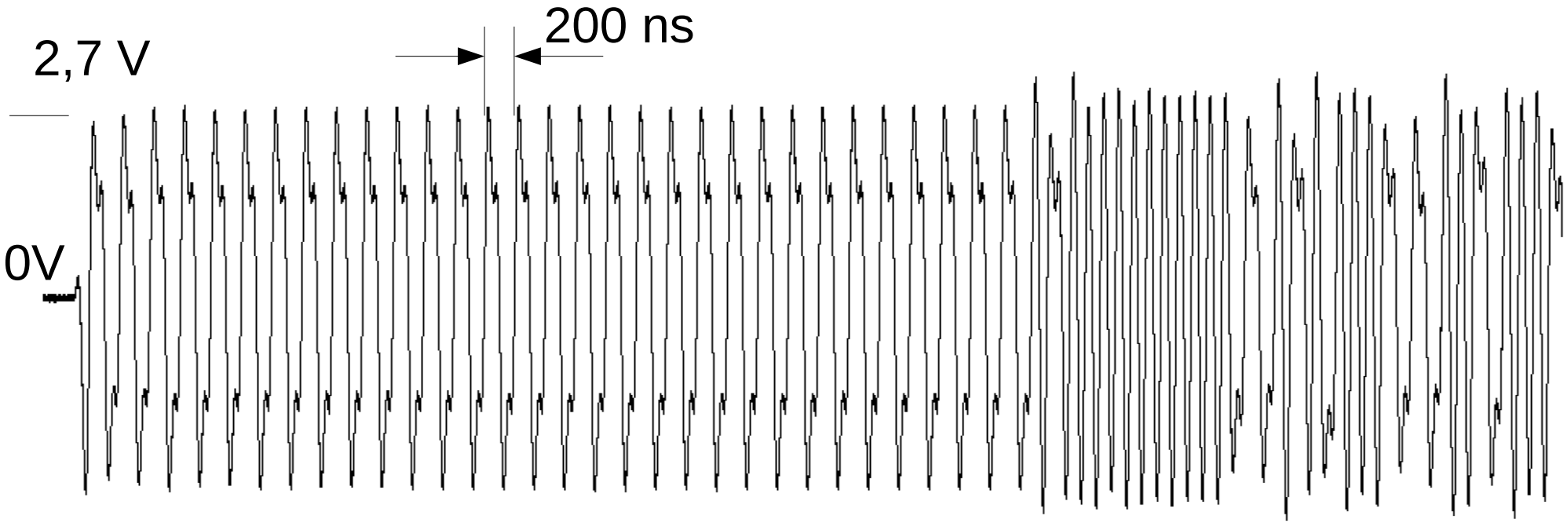
## Le modèle « ethernet/TCP/IP »

Presque ISO !



# Début de trame Ethernet 10 Mbps

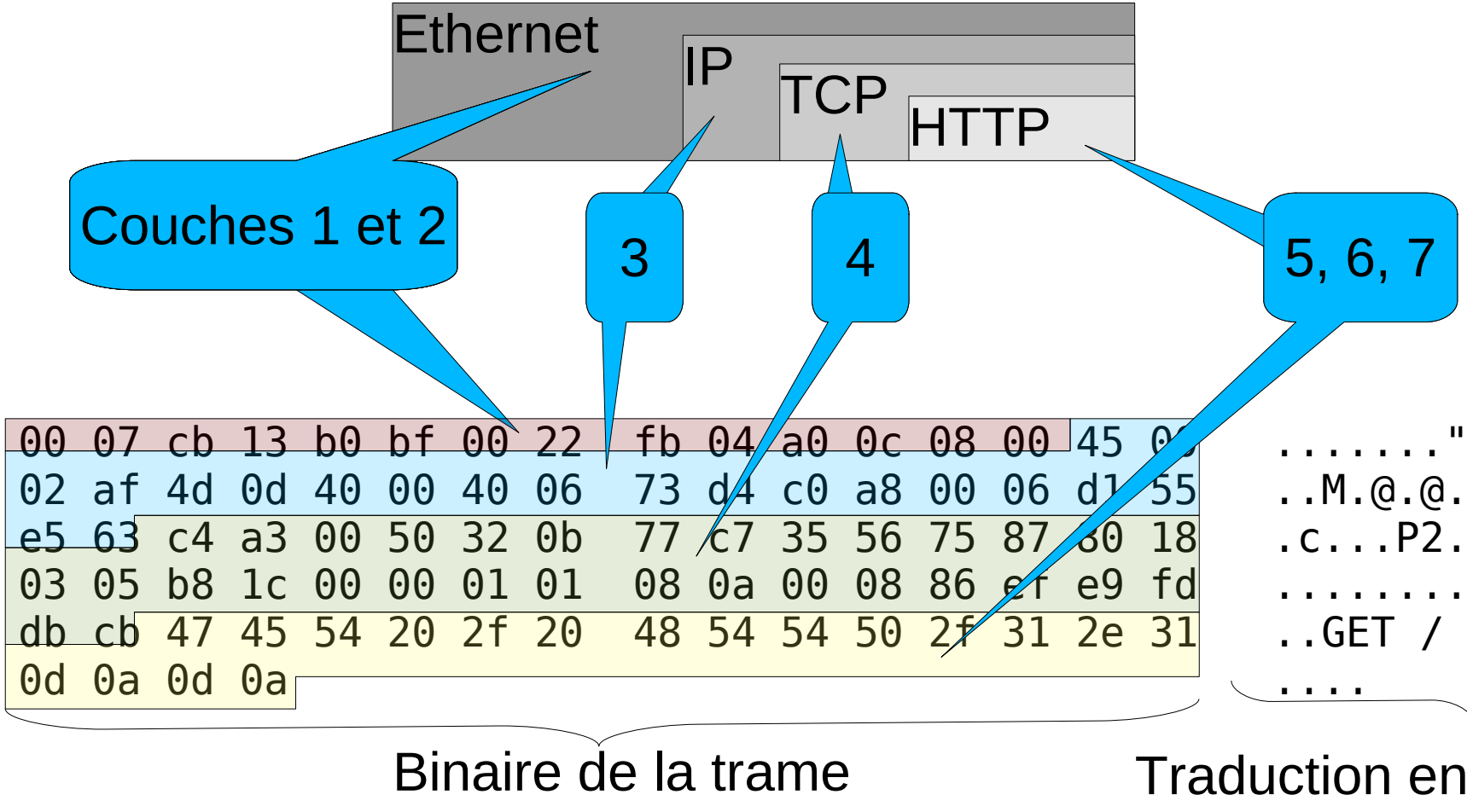
0 : front descendant
1 : front montant
Les octets sont représentés au format LSB d'abord et les champs au format MSB d'abord.




| Synchro | SFD | Adresse destination | ... |
|---|---|---|---|
| 10101010...10101010 | 10101011 | 00000000 00001011 00111101 | |
| | | 00 D0 BC | |

# Le modèle Ethernet – IP

Exemple d'une requête envoyée par un navigateur (demande la page d'accueil de Google à partir d'un PC connecté à une Freebox)



# Les couches basses

**PLAN**

1.Topologie

2.Les méthodes d'accès au média

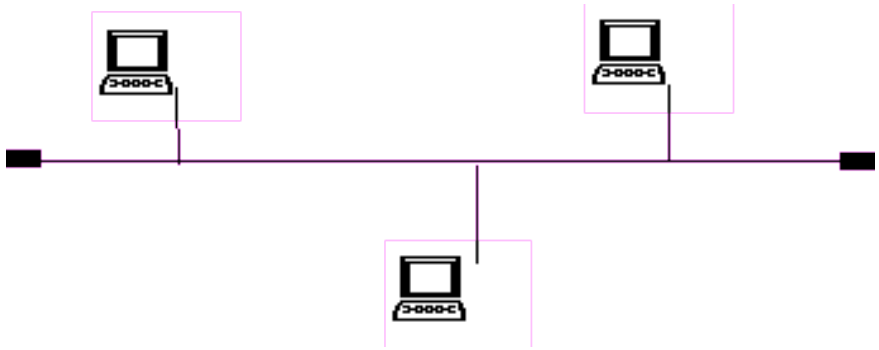
3.Ethernet

# Topologie

2 types de topologie:
Physique: la forme du maillage physique (câbles à l'intérieur d'un bâtiment)
Logique: la forme "que voit le protocole".

**Topologie en bus**
- simple
- diffusion naturelle des trames

**mais**
- localisation des pannes difficile
- collisions de trames



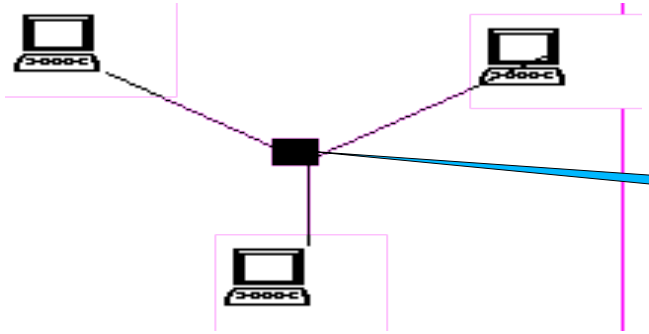
C'est la topologie des réseaux embarqués : CAN bus, LIN bus, 1-wire ®, I2C ®

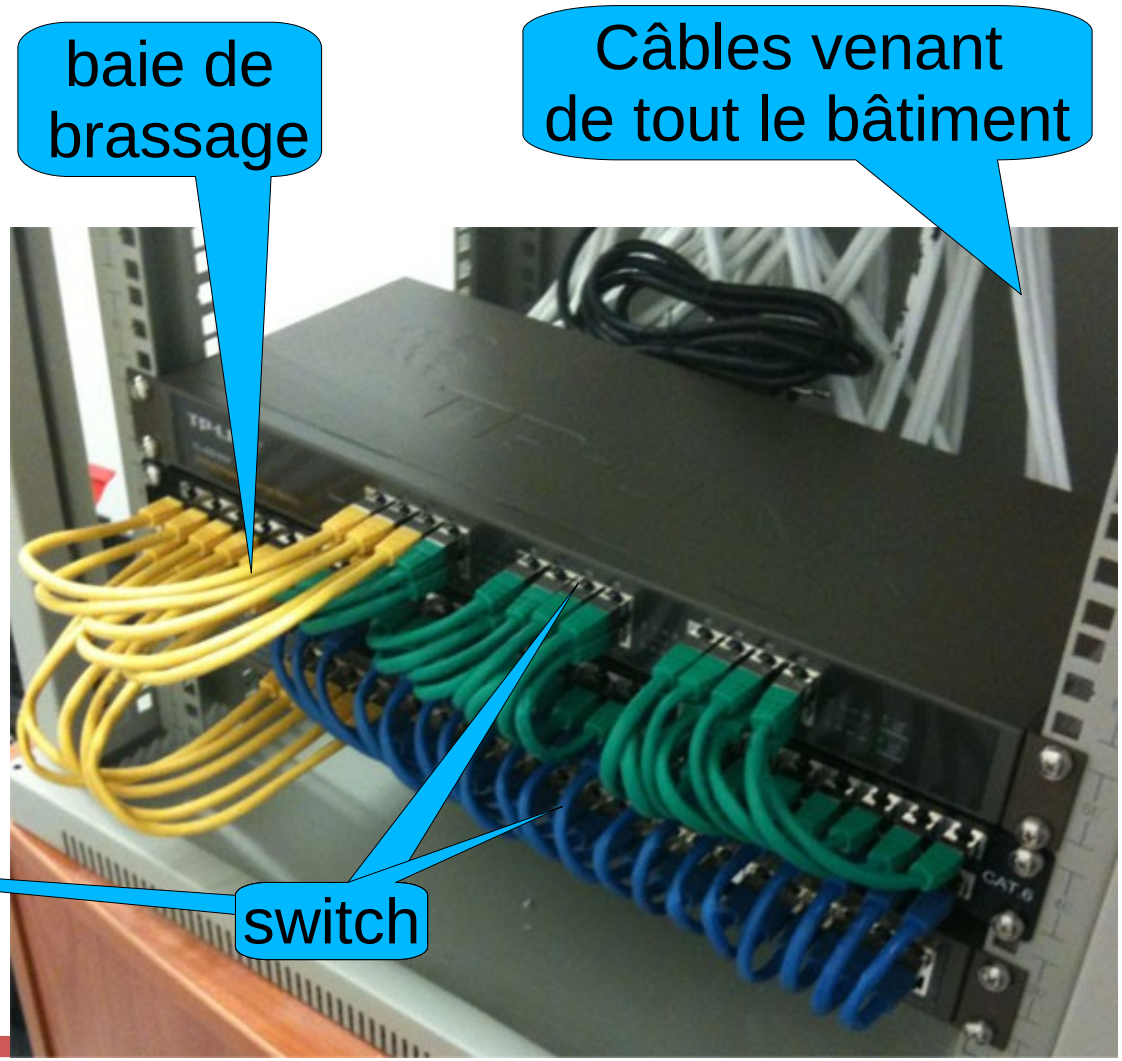
# Topologie

**Topologie en étoile**

– Pannes faciles à détecter
– Administration centralisée
**mais**
– Nécessite souvent un pré-câblage

→ utilisé dans les réseaux tertiaires.





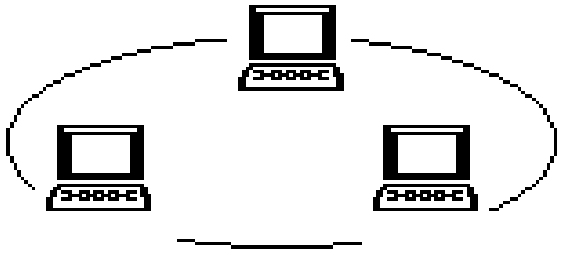
# Topologie

**Topologie en anneau**

- une trame particulière circule sur le réseau toujours dans le même sens
- quand une machine veut émettre :
  - → attendre de recevoir le jeton ;
  - → émission d'une trame de données à la place du jeton ;
  - → le destinataire modifie la trame pour indiquer qu'il l'a bien reçue ;
  - → quand la trame a fait le tour, réémission du jeton.

régénération du signal électrique
protocole simple : pas de collision.

**Mais**
pb en cas de rupture d'un câble
câble 2 fois plus long qu'en topologie bus



# Les méthodes d'accès

**Dans tous les cas, nécessité d'un adressage si plus de 2 machines !**

Point à point : liaison série.

Maitre / Esclave avec gestion du tour de parole : CPU sur un bus

Arbitre (résolution en cas de conflit) : Point d'accès Wifi

Détection de porteuse avec résolution des collisions : Ethernet

Détection de porteuse avec évitement des collisions : Bus CAN

Multiplexage : par insertion dans des wagons temporels et/ou fréquentiel. Sur-tout utilisé sur fibre optique.

# Ethernet

## Introduction

- Inventé par Xérox dans les années 70 puis normalisé en 83.
- Norme IEEE 802.3
- Topologie logique : Bus  à diffusion naturelle
- Topologie physique : Bus, mais aussi étoile.
- Débit : 10 Mbps théorique, mais plus faible dans la pratique à cause des collisions.
- Codage : 10 MHz, Manchester Différentiel.
- Évoltion vers les hauts débits avec Fast Ethernet et Gigabit Ethernet.

# Switch Ethernet

•Comme un hub mais le switch **ne répète la trame émise que sur les ports concernés**. Plusieurs machines peuvent parler en même temps.

•**Apprend la topologie** du réseau ;

•**Full duplex**, jusqu'à 10 Gbps ;

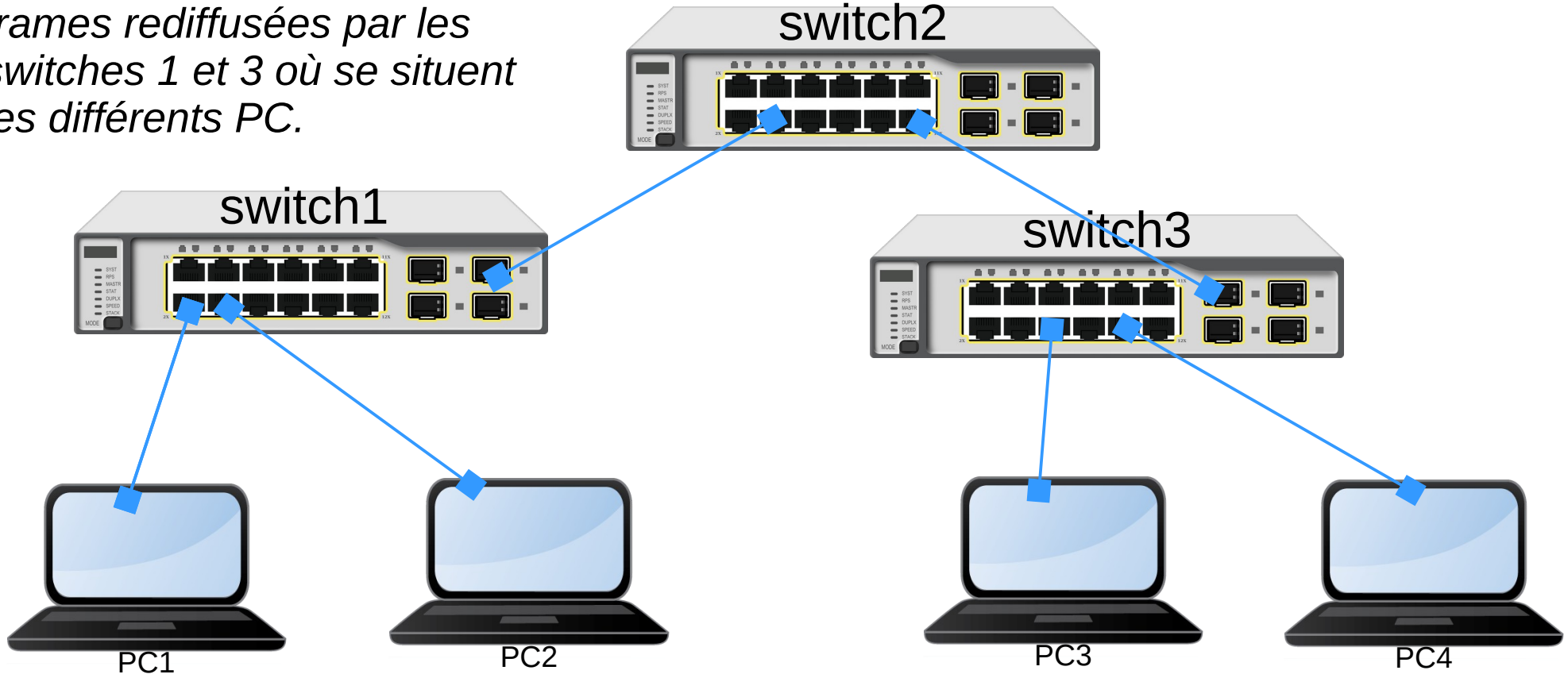
•Protocole STP (**Spanning Tree Protocol**) permettant d'éviter les boucles dans le réseau en cas de maillage de plusieurs switch.

- Il est transporté par ethernet + LLC.
- C'est un protocole permettant d'établir un arbre couvrant à coût minimum entre tous les noeuds du réseau.

# Switch Ethernet

## Auto apprentissage de la topologie du réseau par adresse MAC

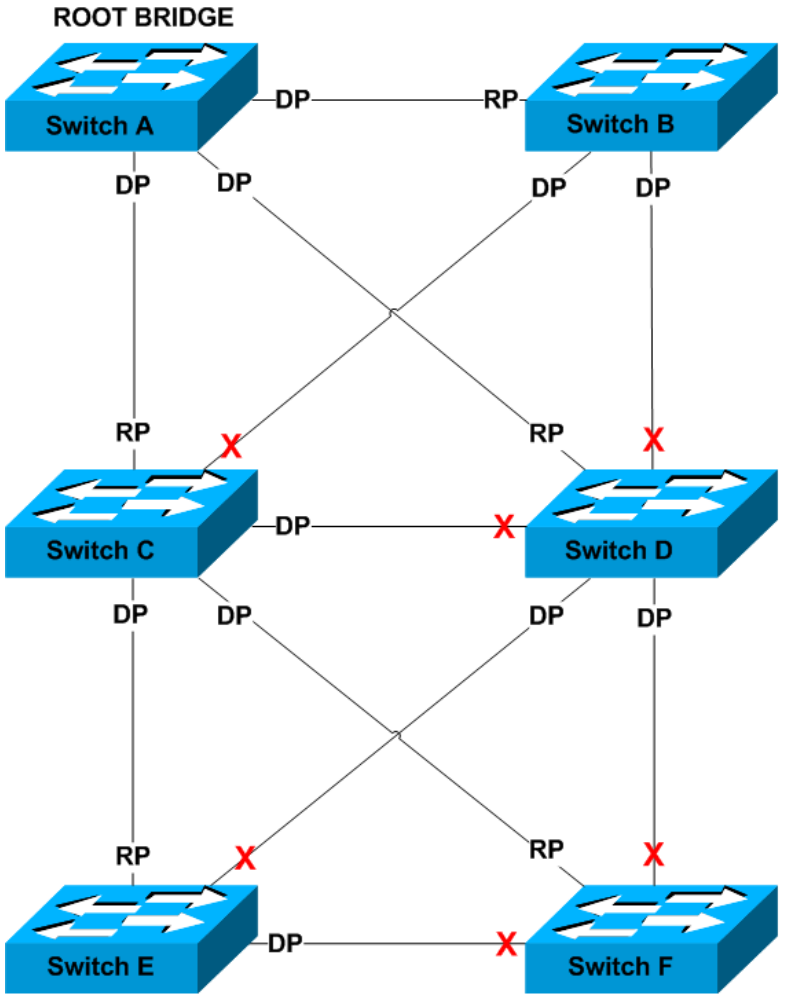
*Par les trames de broadcast (ARP par exemple), le switch 2 apprend par les trames rediffusées par les switches 1 et 3 où se situent les différents PC.*



# Spanning Tree Protocol

Pour augmenter la robustesse du réseau :

- l'administrateur va créer des liaisons redondantes
- pb : des trames vont être dupliquées
- il peut aussi y avoir des tempêtes de broadcast



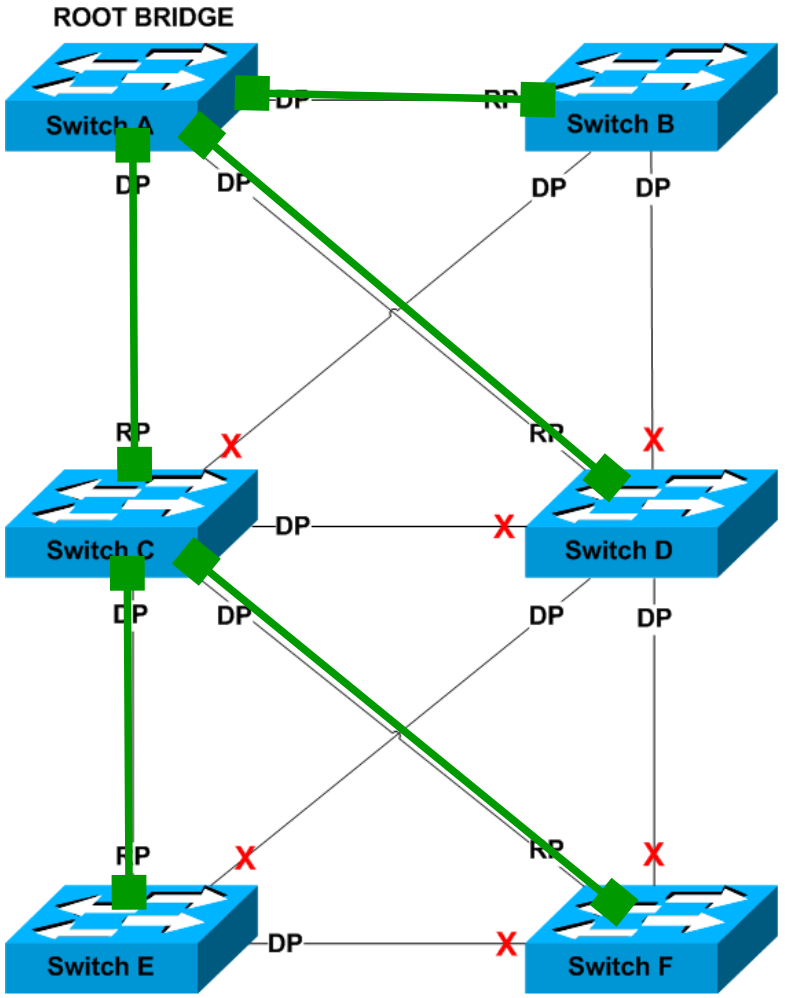
# Spanning Tree Protocol

**Solution :**

établir un Arbre couvrant (en vert)
à coût minimum sur le réseau.

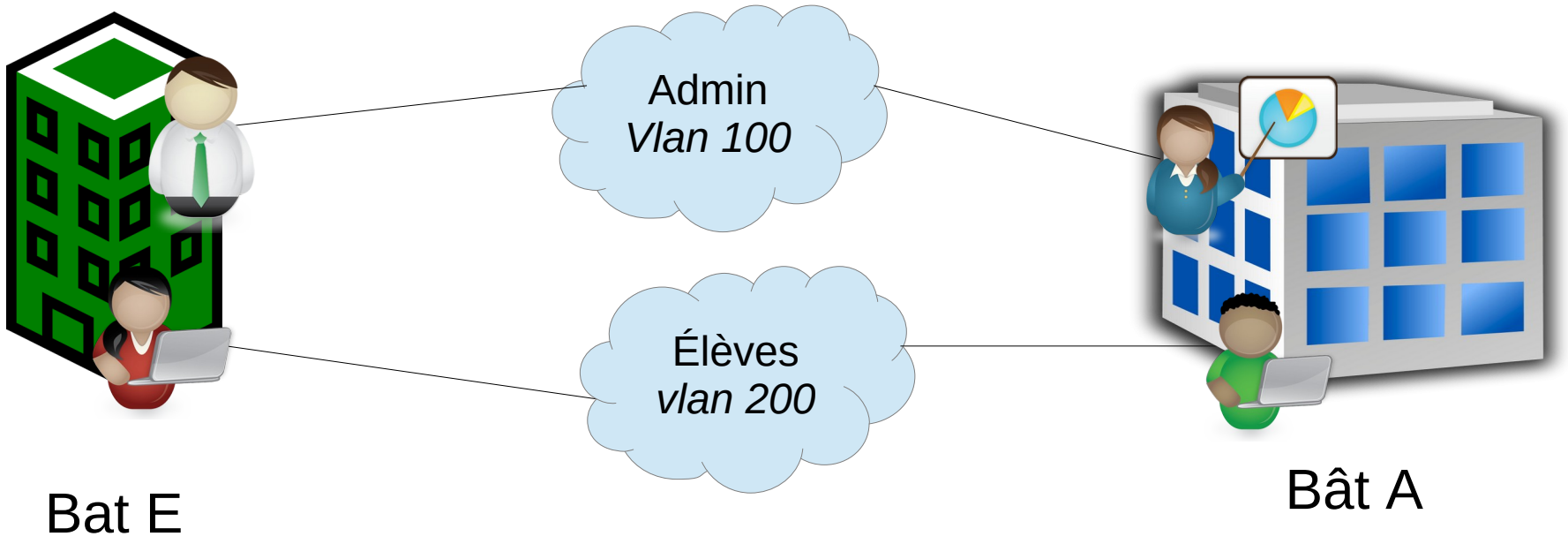
Chemin unique pour atteindre chaque nœud du réseau

Algorithme de spanning tree.

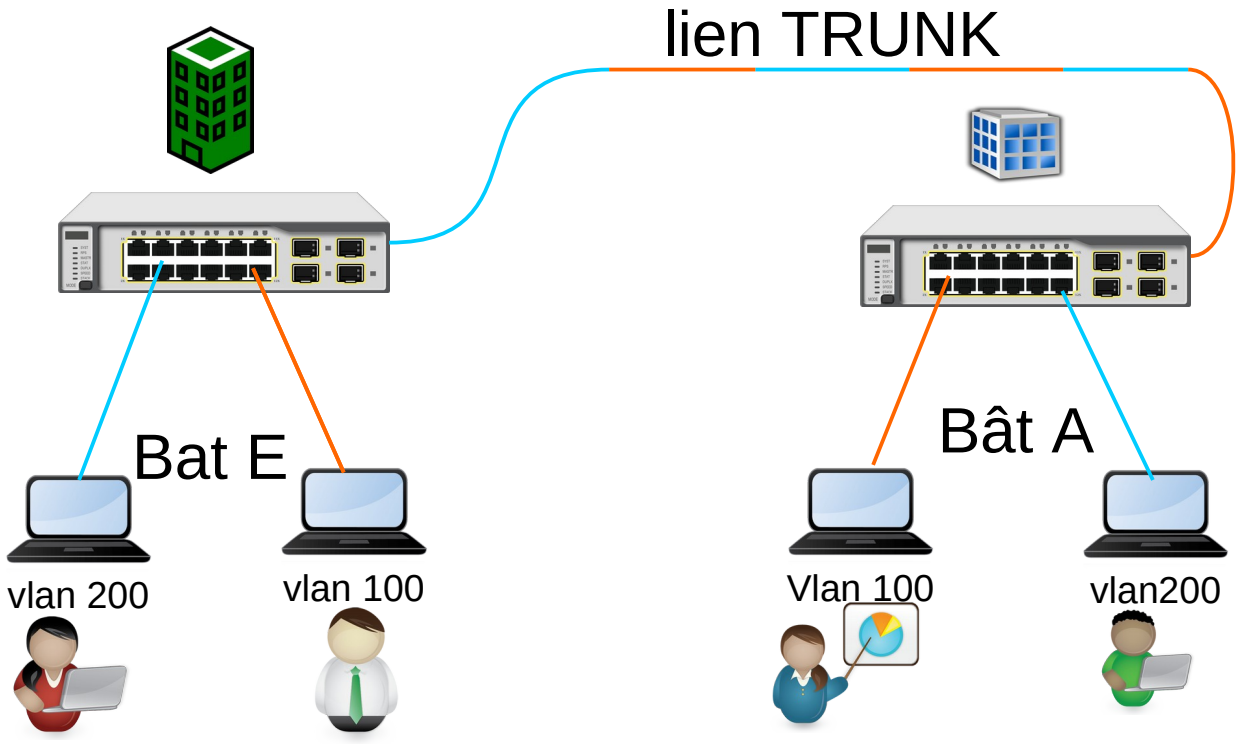


# Virtual LAN

utiliser un même switch MAIS créer des réseaux locaux virtuels étanches



# VLAN



# Switch Ethernet (VLAN)

•Mécanisme de VLAN (Virtual LAN) permettant de simuler plusieurs LAN comme s'ils étaient séparés physiquement.

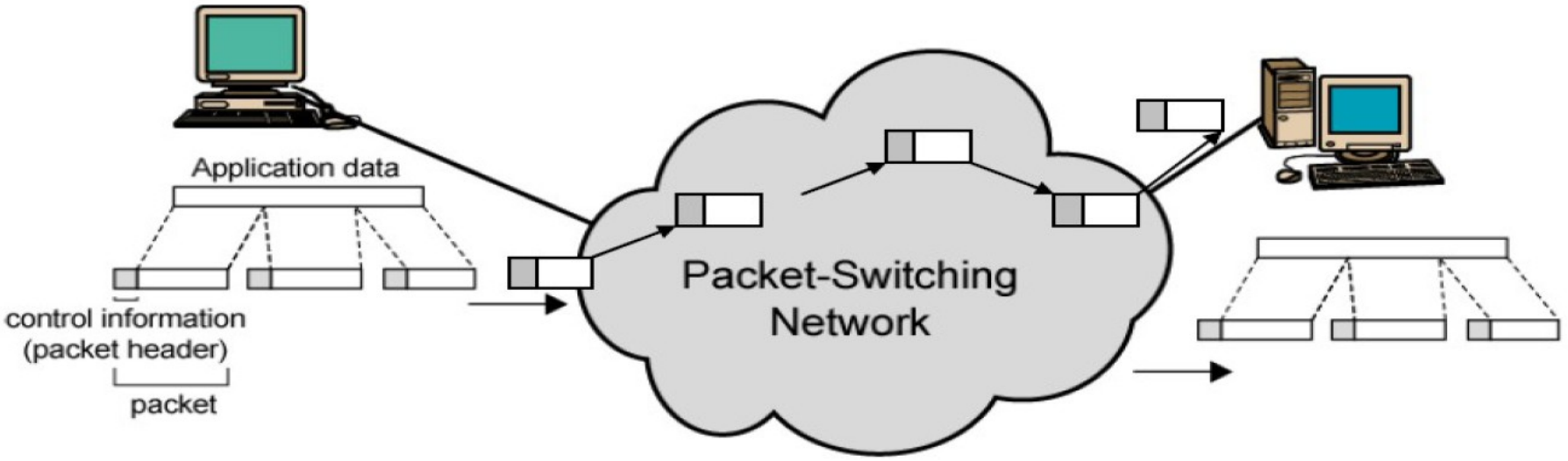
•Le mécanisme le plus courant est le VLAN par port. A chaque port des switches est associé à un VLAN-ID.

•Seules les machines d'un même VLAN peuvent communiquer ensemble.

•Quand une trame sort du switch à destination d'un autre switch (lien trunk) , un champ supplémentaire (tag) est ajouté à la trame ethernet, permettant au switch recevant la trame de savoir de quel VLAN la trame est issue.
•Le tag (4 octets) est inséré juste après l'adresse MAC destination

# Internet Protocol

Une idée simple : des paquets (datagrammes) autonomes !



# IP – 3 types de datagramme

- les **datagrammes de données** : transportent l'information utilisateur ;
- les **datagrammes de contrôle** des données : erreurs réseau...
- les **datagrammes de supervision** du réseau : gestion du routage, maintenance afin de prévenir la congestion...

# IP - Quelles informations dans la trame ?

Quelles informations dans les entêtes des datagrammes:

2 version d'IP : version 4 ou version 6

2 versions **incompatibles** avec des entêtes différentes.

Par exemple :

- Version 4 : adresse sur 32 bits
- Version 6 : adresse sur 128 bits

Le premier champ du datagramme doit permettre de savoir de quelle **version** il s'agit.

# IP - Quelles informations dans la trame ?

Le format de la trame IP (en mots de 32 bits) :

<table>
<tr><td colspan="4">0 1 2 3</td><td colspan="4">4 5 6 7</td><td colspan="8">8 9 10 11 12 13 14 15</td><td colspan="16">16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31</td></tr>
<tr><td colspan="4">N° version</td><td colspan="4">long entête</td><td colspan="8">qualité de service (TOS)</td><td colspan="16">long totale</td></tr>
<tr><td colspan="16">n°de datagramme</td><td colspan="3">flag</td><td colspan="13">frag offset</td></tr>
<tr><td colspan="8">Time to live</td><td colspan="8">Protocole transporté</td><td colspan="16">checksum entête</td></tr>
<tr><td colspan="32">Adresse source</td></tr>
<tr><td colspan="32">Adresse destination</td></tr>
<tr><td colspan="32">... Options ...</td></tr>
<tr><td colspan="32">Données</td></tr>
</table>

# adressage IPv4

- **Une adresse IP** = un numéro sur 32 bits, noté par des octets en base 10 séparés par des point. Ex : 10.7.0.254
- **Un réseau IP** = un ensemble de machines sur un réseau local
- **Un réseau IP** = un espace d'adressage/numérotation **contigu** des machines

  Ex de 192.168.1.0 à 192.168.1.254

# adressage IPv4

Des machines d'un même réseau ont les **premiers bits de leur adresse identiques.**

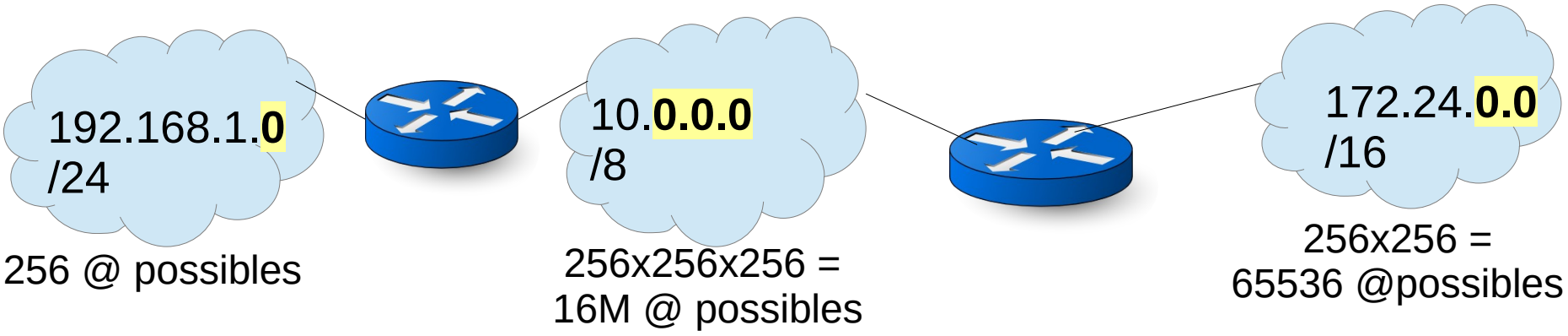
- adresse sur 32 bits
- Limite donnée par netmask
- notation du netmask soit par un « slash » soit en décimal pointé.

Exemple /24 == 255.255.255.0

| | Net ID | Host ID |
|---|---|---|
| adresse IP : | $n_0n_1n_2n_3$…….. | ….$n_{31}n_{32}$ |
| netmask : | 111….11111 | 00….000 |

32 bits

# IP - Quelles informations dans la trame ?



# adressage IPv4

- Dans l'espace d'adressage du réseau :
  - 1ère adresse réservée au « nom du réseau »
  - dernière adresse réservée au broadcast

- Exemple : A quel réseau fait partie la machine 3.4.5.6/23 ?

# adressage IPv4

Exemple : A quel réseau fait partie la machine 3.4.5.6/23 ?

3.4.5.6 == 0000 0011 . 0000 0100 . 0000 0101 . 0000 0110

/23 == 1111 1111 . 1111 1111 . 1111 1110 . 0000 0000

DONC

@reseau == 0000 0011 . 0000 0100 . 0000 0100 . 0000 0000

@reseau == 3.4.4.0

Nombre de machines dans ce réseau : $2^{(32-23)}$ -2 = 510

@ de broadcast dans ce réseau : 3.4.5.255

# adressage IPv4

Des adresses réservées :

– **127.0.0.0 /8** : communication interne à une machine (entre programmes). 127.0.0.1 est en général utilisé

**- 10.0.0.0/8** (10.0.0.0 – 10.255.255.255) - RFC 1918 : 16 777 216 IPv4

**- 100.64.0.0/10** (100.64.0.0 - 100.127.255.255) - RFC 6598 : 4 194 304 IPv4

**- 172.16.0.0/12** (172.16.0.0 – 172.31.255.255) - RFC 1918 : 1 048 574 IPv4

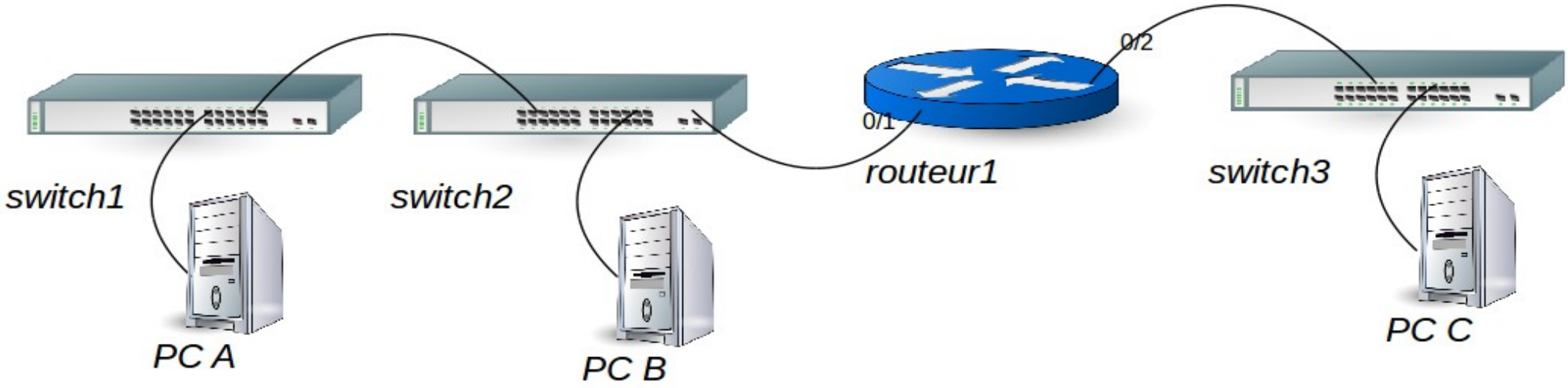
**- 192.168.0.0/16** (192.168.0.0 – 192.168.255.255) - RFC 1918 : 65 536 IPv4

adresses **privées** réservées à un usage interne. Les machines avec ce type d'adresse doivent passer par une passerelle de type proxy ou NAT pour avoir accès à internet.

– **224.0.0.0 /24** : adresses de multicast réservées à la communication de groupe.

# acheminement local / global
# Ex : Ethernet

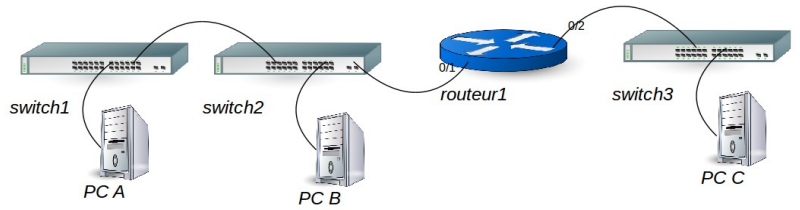
Voici le schéma physique d'un réseau




1 -Dessinez le schéma logique

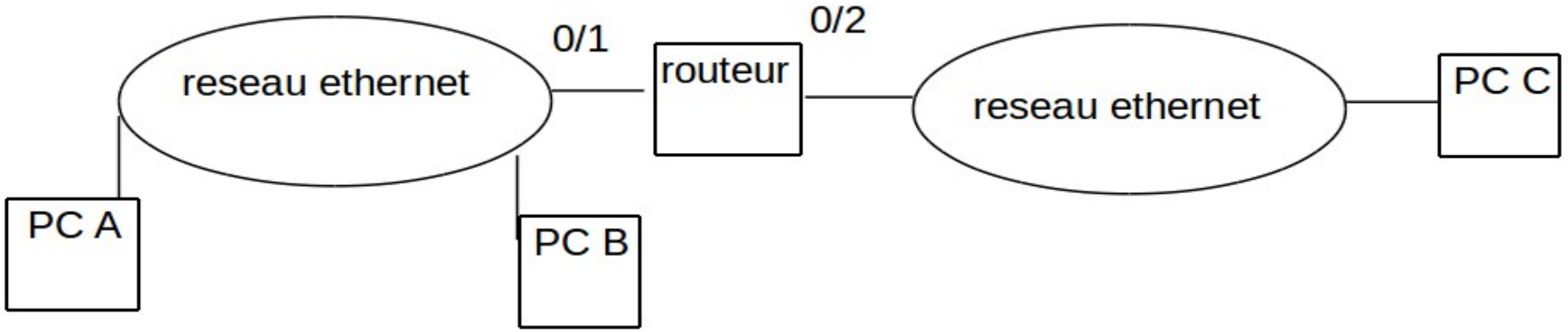
# acheminement local / global
# Ex : Ethernet

Voici le schéma physique d'un réseau



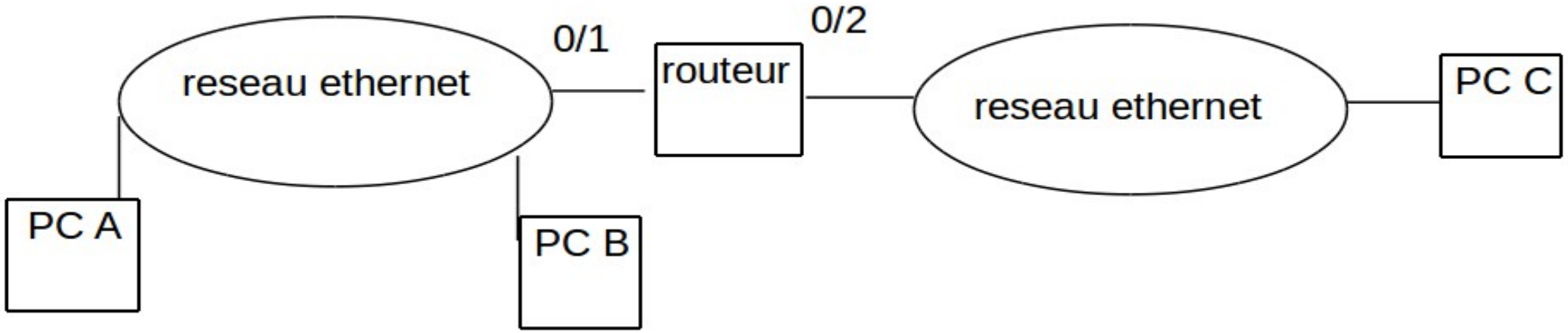

1 -Dessinez le schéma logique

Schéma Logique



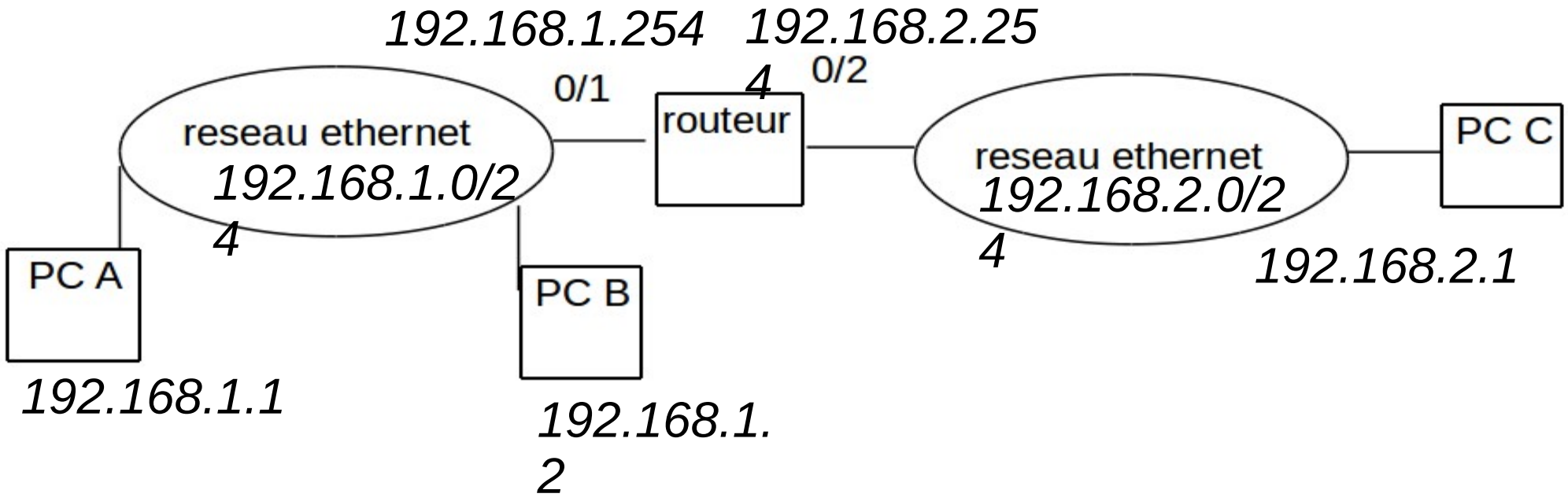
# acheminement local / global
# Ex : Ethernet

2 - Donnez des adresses aux machines parmi 192.168.0.0/16

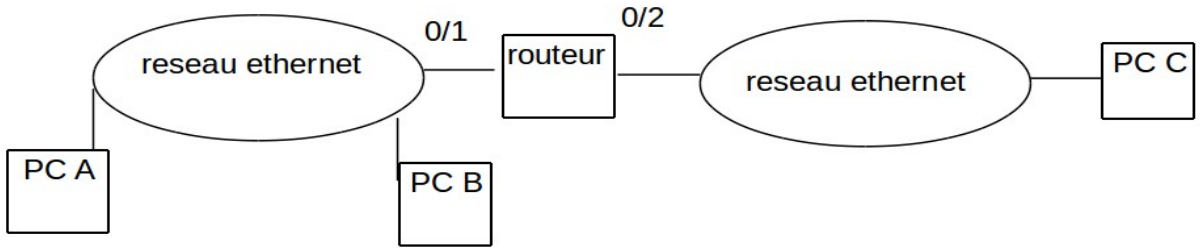


# acheminement local / global
# Ex : Ethernet

2 - Donnez des adresses aux machines parmi 192.168.0.0/16



# acheminement local / global
# Ex : Ethernet




3 – Complétez le schéma suivant

| | Adresse MAC source | Adresse MAC destination | Adresse IP source | Adresse IP destination |
|---|---|---|---|---|
| Trame de A vers B vue de B | ***@MAC de A*** | ***@MAC de B*** | ***@IP de A*** | ***@IP de B*** |
| Trame de A vers C vue de A | ***@MAC de A*** | ***@MAC de 0/1*** | ***@IP de A*** | ***@IP de C*** |
| Trame de A vers C vue de C | ***@MAC de 0/2*** | ***@MAC de C*** | ***@IP de A*** | ***@IP de C*** |

# Attribution des adresses

Une machine doit connaître :

- son adresse IP
- netmask
- passerelle
- @IP du DNS
- Éventuellement le domaine d'interrogation du DNS par défaut. Par exemple si le domaine est « ensicaen.fr », pour un utilisateur qui cherche à joindre « cybele », la requete au DNS sera « quelle est l'adresse IP de cybele.*ensicaen.fr* »

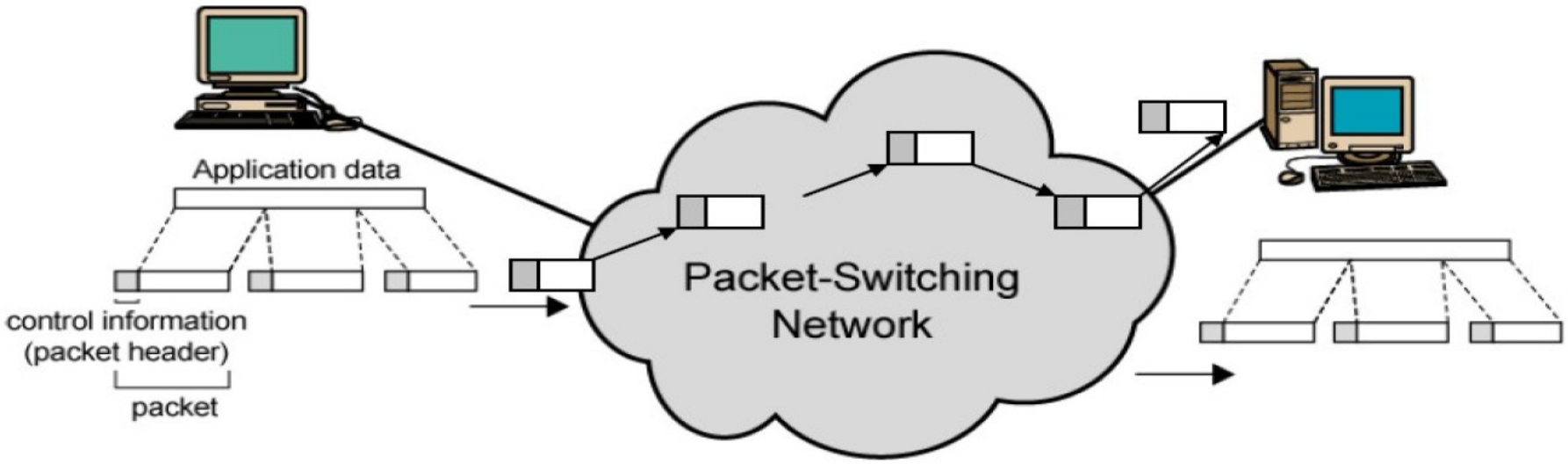
*remarque l'adresse MAC est une caractéristique intrinsèque de la carte réseau (wifi/ethernet/bluetooth…).*

# Couche Transport

Transporter l'information de bout en bout en assurant :

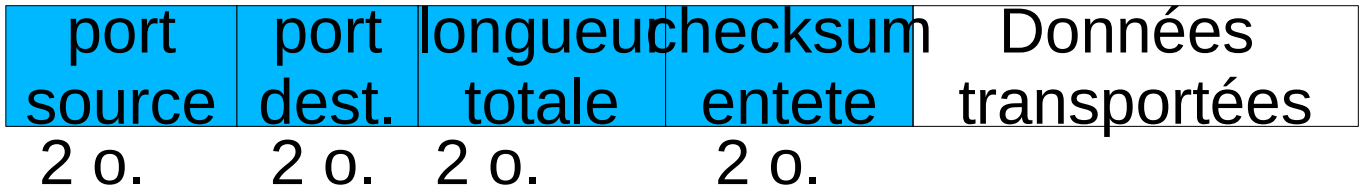
- la remise de l'information à la bonne application : n° de port
- le contrôle (détection / récupération) ou non des erreurs

**→ 2 protocoles : UDP, TCP**



# UDP

- User Datagram Protocol
- Non fiable
- Entête :




- Longueur maximale des données transportées :
  - MTU IP – long entete IP – entete UDP
  - soit 1500 – 20 – 8 = 1472 sur Ethernet.
  - Le reste peut être tronqué par UDP selon les implémentations.

# UDP

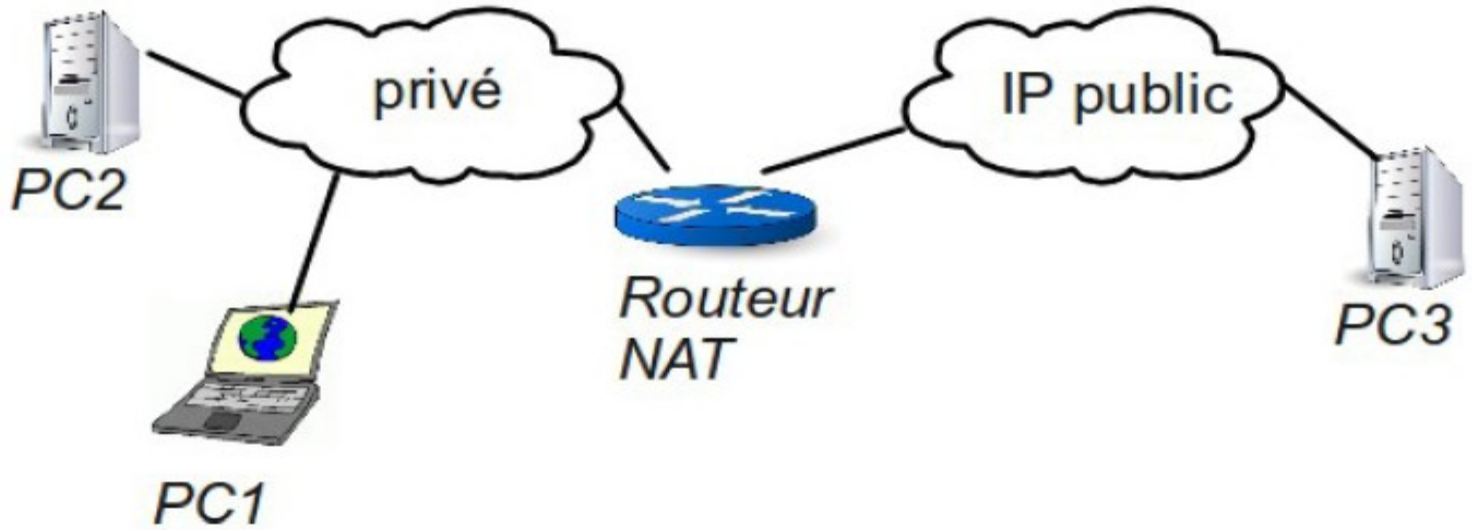
- Utilisé pour des **services simples**.
- Par exemple : DNS (port 53) , DHCP (port 67) , TFTP (port 69)
- Ou pour des services pour lesquels la reprise sur erreur arriverait trop tard comme en **téléphonie**.
- On distingue le **client** qui envoie la requête ;
- Et le **serveur** qui répond.
- Le **serveur** doit être lié à un **port connu à l'avance** par le client. Ces ports sont répertoriés pour les services classiques : 53 pour DNS, 67 pour DHCP...
- Le port du **client** est choisi par le système d'exploitation parmi les **ports libres**.

# TCP

- Transmission Control Protocol
- **Transport Fiable** :
  - les paquets sont numérotés ;
  - les paquets **non acquittés en temps utile sont envoyés de nouveau**
  - l'application n'a pas à ce soucier de la gestion des erreurs. TCP s'en charge.
- Permet le **contrôle de flux**.
- Comme en UDP on distingue le **client** et le **serveur**
- Le **serveur** doit être lié à un **port connu à l'avance** par le client. Ces ports sont répertoriés pour les services classiques : 21 pour FTP, 80 pour HTTP...
- Le **port du client** est choisi par le système d'exploitation parmi les **ports libres**.

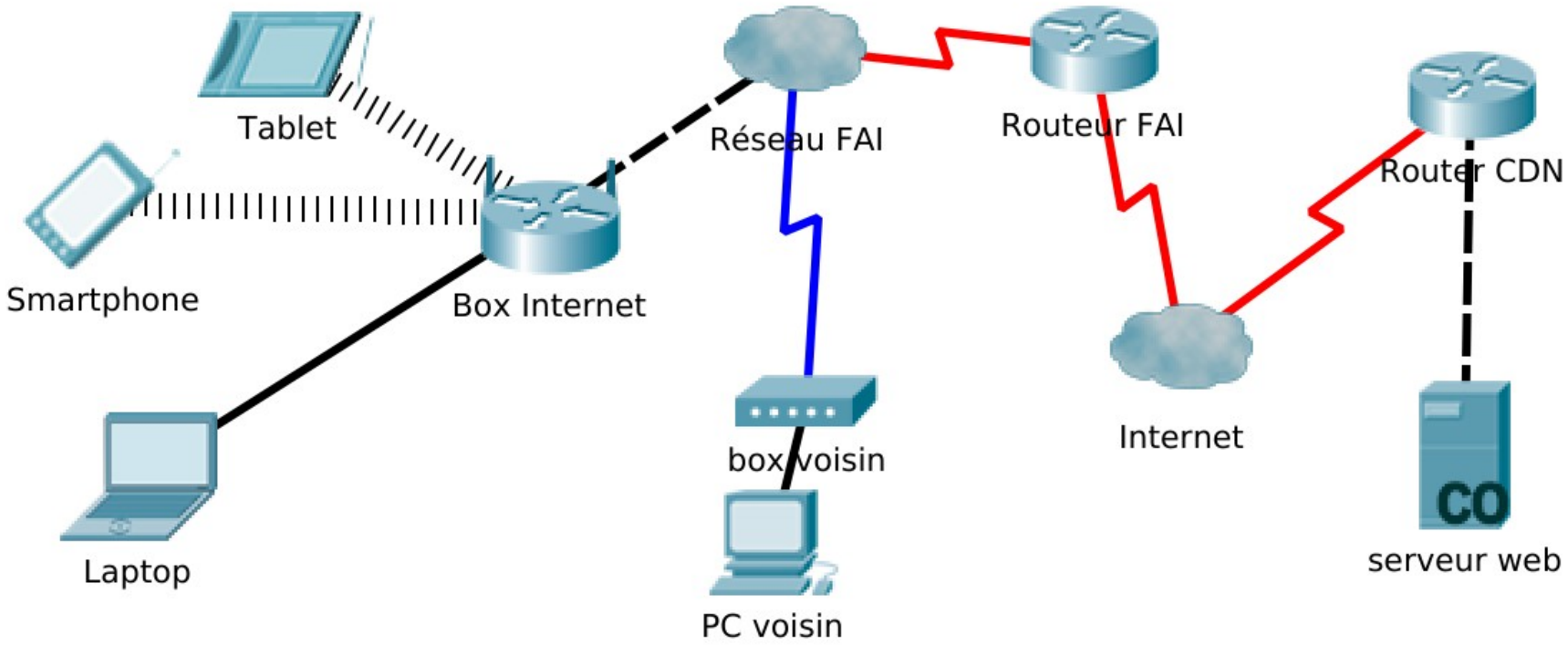
# NAT / PAT

- Network Address Translation / Port Address Translation
- Pour faire face à la pénurie d'adresses IP et partager une connexion internet (c'est ce que faitune box ASDL)
- Mais aussi pour contrôler ce qui sort sur l'internet public (Toutes les connexions data sur réseau GSM et dérivés utilisent ce principe).
- Ci-dessous le routeur transforme les @ privées en @ publique (souvent unique)



# NAT / PAT

- Double NAT




- La box « NAT » les adresses… le routeur du FAI peut également le faire…

# Sécurité

La sécurité des données consiste à garantir un ou plusieurs des objectifs suivants :

- L'**intégrité :** assurer que les données n'ont pas été altérées.
- La **confidentialité** : assurer que les données ne peuvent être lues que par des personnes autorisées.
- La **disponibilité** : assurer que les données sont accessibles 24h/24.
- La **non répudiation** : assurer que l'émetteur des données ne peut nier en être l'auteur.
- L'**authentification**, assurer que les parties ayant accès à l'information sont connues (au sens civil).

***→ Le réseau n'est qu'un maillon de la chaîne !***

# Sécurité

***La sécurité du système d'information :***

- c'est l'affaire de tous :
  - avoir des mots de passe solide
  - savoir reconnaître un mail de « phishing »
  - lutter contre les logiciels malveillants (venant d'une clé USB ou d'un site web…)
  - connaître les bonnes pratiques du paiement sécurisé.
  - avoir des systèmes d'exploitation et des logiciels à jour.

- Difficile de donner des chiffres, mais un coût réel pour l'entreprise. On parle d'une moyenne de 700 000 € par attaque et 9 semaines* pour s'en remettre :
  - perte d'image
  - frais juridiques
  - compensation clients….


** source NTT Com Security 2016*

# Sécurité

C’est du **bon sens**, de la **rigueur** et des connaissances à jour.

En France, l’Agence nationale de la sécurité des systèmes d’information – **ANSSI** – accompagne les entreprises par des actions de conseil et de réglementation :

- formation des personnels
- mise en place de firewall
- méthodes de chiffrement
- alertes de sécurité (notamment systèmes…)
- mise en place de PSSI : politiques de sécurité des systèmes d’information

# Chiffrement des données

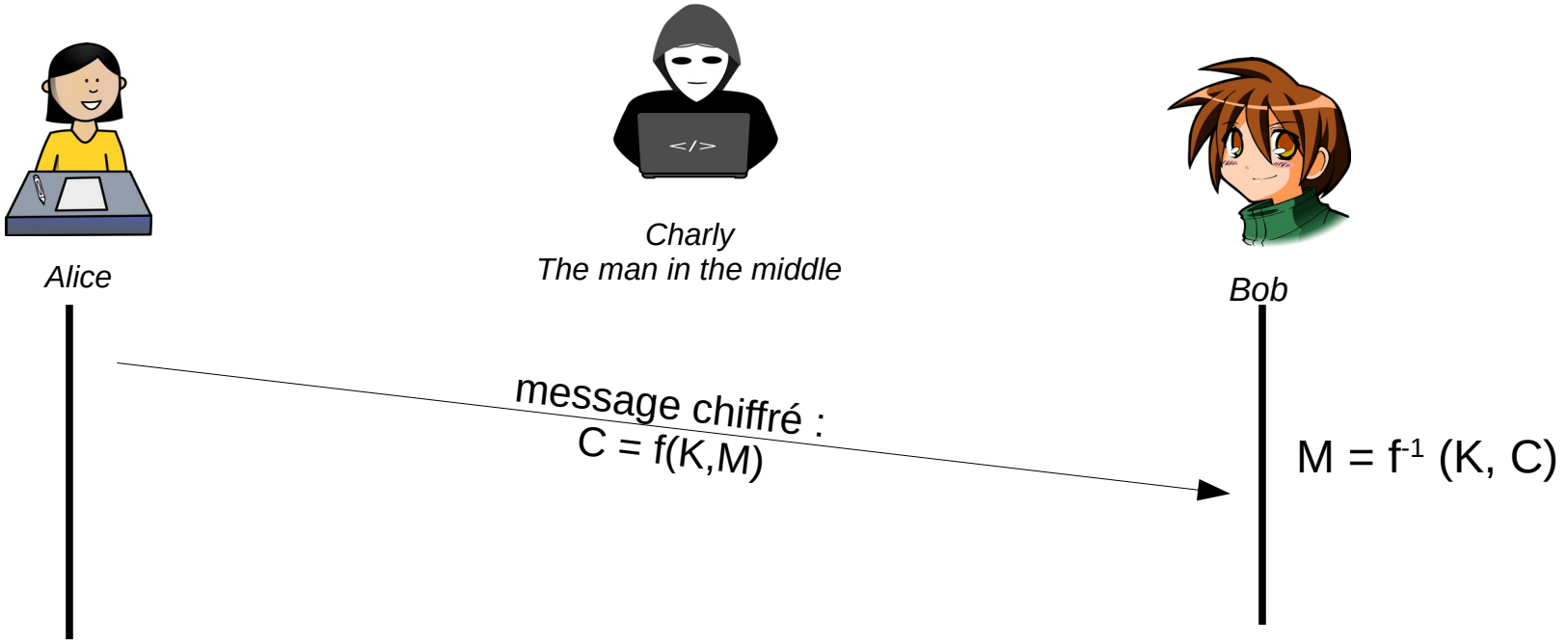
Pour sécuriser les données on a recourt au chiffrement (ou « cryptage »)
qui consiste à **transformer** les données.

L'opération de chiffrement peut présenter plusieurs caractéristiques :

- **inversible** ou non
- rapide ou nécessitant de longs temps de calculs
- **symétrique** (la même clé sert au codage et au décodage)
- ou **asymétrique** : existence de 2 clés.

*Enigma*

# Chiffrement symétrique




- f : algorithme de chiffrement : en général connu
- M :  message à chiffrer
- K : clé de chiffrement secrète connue uniquement de Alice et Bob
- C : message chiffré

# Chiffrement symétrique

Exemple de code simple symétrique le codage par substitution :

Un symbole (un caractère par exemple) est substitué par un autre symbole selon une règle qui dépend d'une clé.

Exemple de règle simpliste : on remplace un caractère dont le code ASCII est N par le caractère de code ASCII $(N+C_i)\%256$ (appelé chiffrement de Vigenère)

$C_i$ est un des code ASCII de la clé.

- Par exemple avec le message « Bonjour le monde » et la clé « 12345 » (on suppose que le code ASCII de 1 est 1, celui de 2 est 2... pour plus de simplicité.

```
  Bonjour le Monde
+ 1234512345123451
------------------
  Cqqntvt#pj!Orrif = Message chiffré.
```

- Le décodage est évident.

# Chiffrement symétrique

Dans l'exemple précédent :

- Un symbole n'est pas toujours remplacé par le même symbole ( il a fallu attendre 1853 pour casser le chiffre de Vigenère)
- L'algorithme est simple et donc ne demande que peu de ressource CPU

**MAIS**

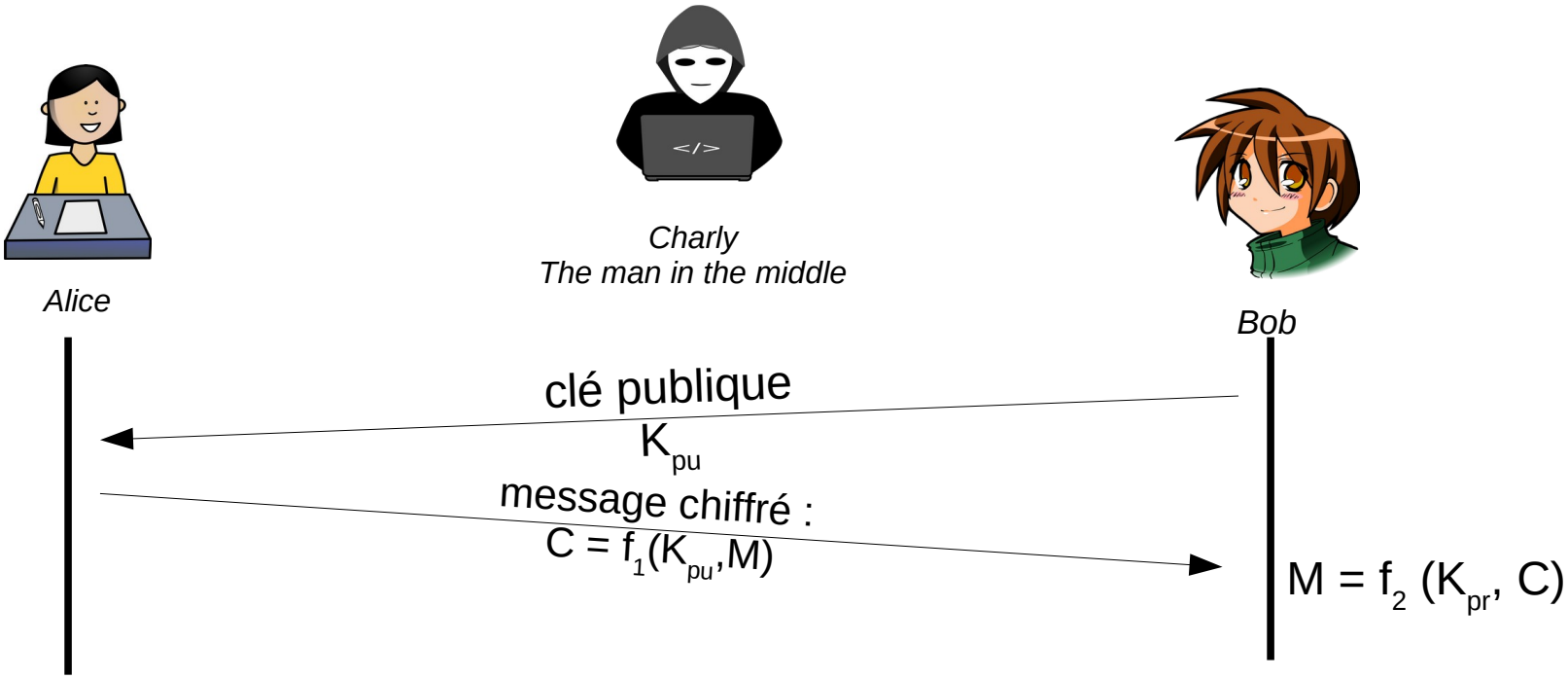
- Par attaque statistique, on peut retrouver la longueur de la clé : L' «espace» va produire des codes dont la fréquence sera élevée. Le « e » aussi...
- Puis connaissant la longueur, on peut faire une analyse statistique des fréquences d'apparition d'un code et supposer qu'il code telle lettre.

→ Des algorithmes symétriques **robustes** et **rapides** existes : **AES** avec des clés de 128 ou 256 bits (AES est approuvé par la NSA... euh, ça veut dire quoi?)

*Remarque DES a été abandonné car sa clé de 56 bits était trop faible.*

- Comment Alice et Bob se sont-ils échangés la clé ?
- Et si N machines doivent s'échanger des données, il faut N*(N-1)/2 clés...

# Chiffrement asymétrique




- $f_1$: algorithme de chiffrement, $f_2$ algorithme de déchiffrement
- M : message à chiffrer
- $K_{pu}$: clé de chiffrement publique de Bob
- $K_{pr}$: clé de déchiffrement privée de Bob (inconnue des autres)
- C : message chiffré

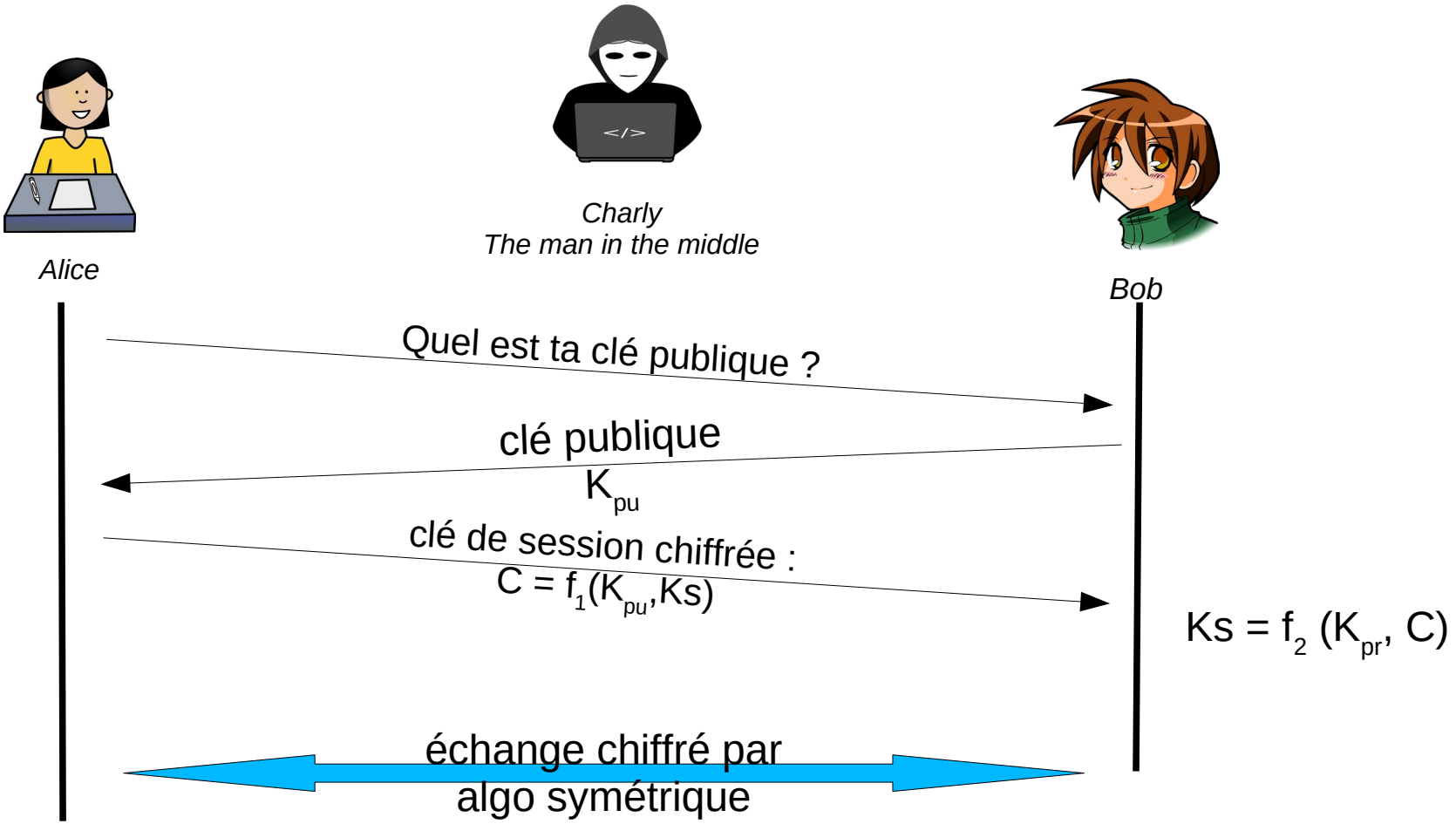
# Chiffrement asymétrique

Les algorithmes $f_1$ et $f_2$ sont en général connus.

- Connaitre $K_{pu}$ ne révèle rien sur $K_{pr}$
- Algorithme le plus utilisé : RSA du nom des inventeurs Rivest Shamir Aldleman alors étudiants au MIT.
- Basé sur le fait qu'il est difficile de décomposer un grand nombre (2048 bits) en facteurs premiers surtout si ce grand nombre est le résultat de la multiplication de seulement 2 nombres premiers.
- Utilise le petit théorème de Fermat : *http://villemin.gerard.free.fr/Wwwgvmm/Decompos/DivisiFe.htm*
  - On admet que si p est premier $(n^p)\%p = n\%p$ On dit ausi que $n^p$ est congru à $n$ , modulo $p$.
  - Cela veut dire que $n^p = n + k.p$ ou encore $n.n^{p-1} = n + k.p$ ou encore $n.(n^{p-1} – 1) = k.p$
  - Donc si n et p sont premiers entre eux (n et p sont étrangers)
  - on déduit si dessus que $(n^{p-1} – 1)$ est divisible par p donc : $n^{p-1} - 1= k_2.p$ noté

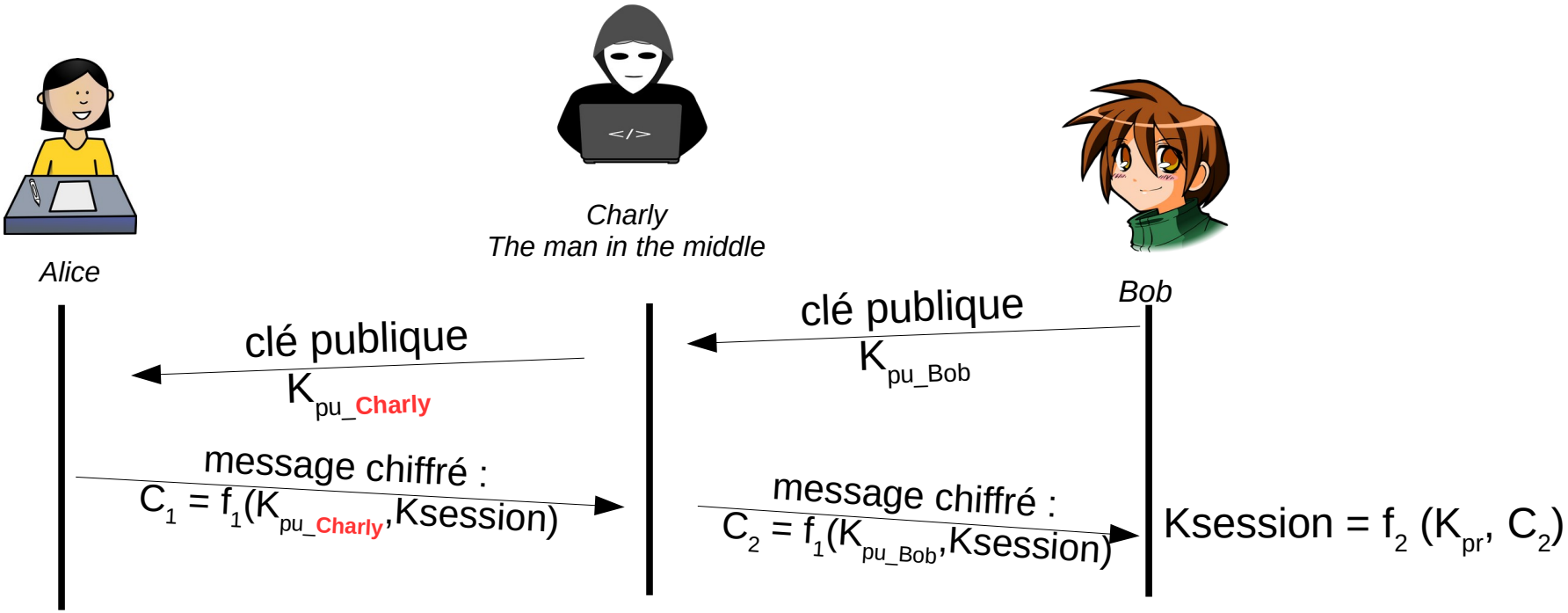
  **$n^{p-1} \equiv 1 \bmod p$**

# Chiffrement asymétrique + clé de session symétrique




- Le chiffrement asymétrique est lent : mieux vaut utiliser un chiffrement symétrique dont la clé sera échangée par cheffrement asymétrique

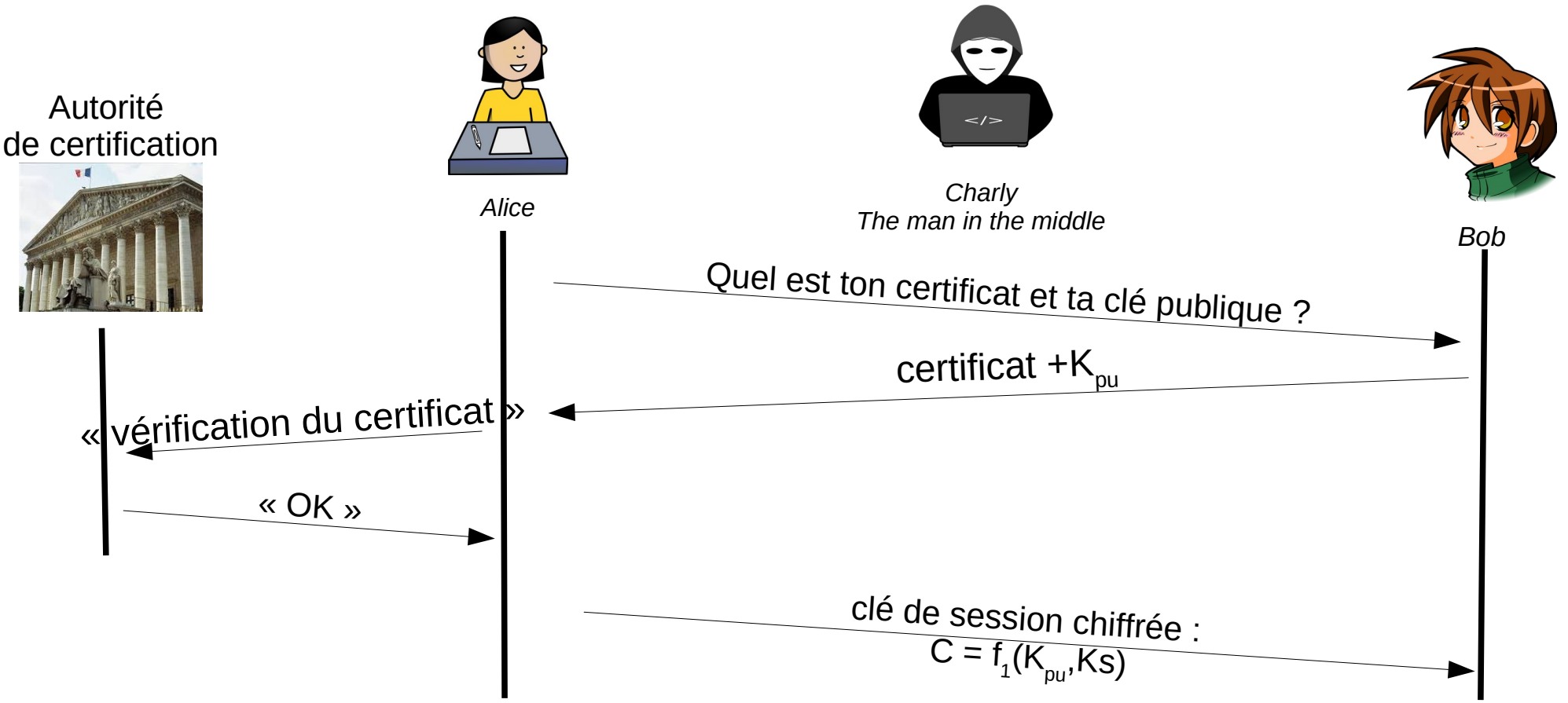
# Certificats




- Charly vient d'intercepter la clé de session entre Bob et Alice… il va pouvoir tranquillement écouter la communication !
- Comment Alice peut-elle être sure qu'elle vient de recevoir la clé de Bob ?
- En plus, Bob ne s'en rend pas compte….

# Certificats

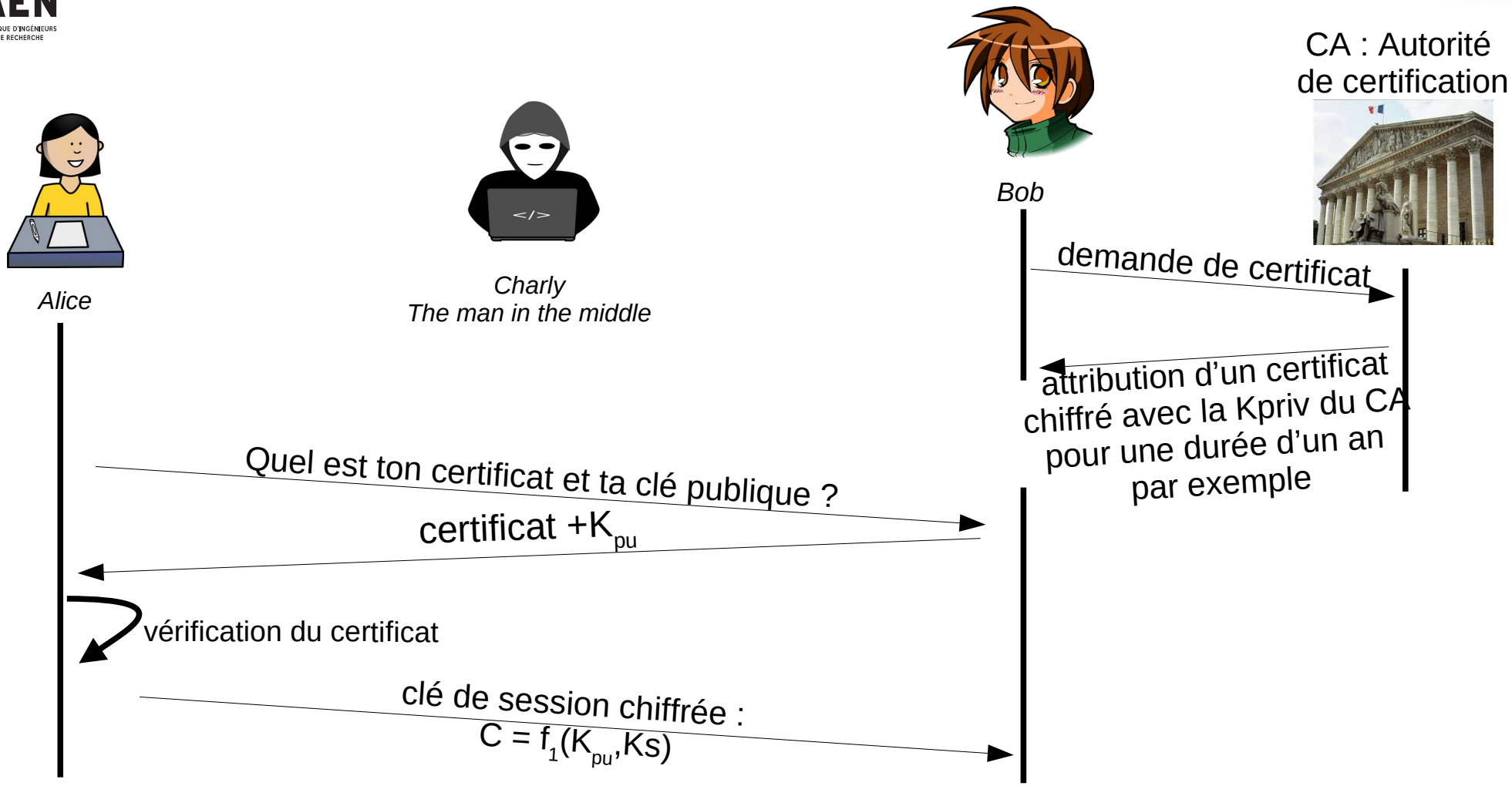
## Une solution...




– Comment Alice sait-elle qu'elle dialogue avec l'autorité de certification ?

*Autorité de certification connue : Thawte, Verisign...*

# Certificats




Alice ne va pas dialoguer directement avec le CA “Certificate Authority” mais grâce à la clé publique du CA stockée sur sa machine, elle va pouvoir vérifier l’authenticité du certicicat de Bob.

# Signature numérique

- permet de garantir l'authenticité de l'expéditeur ;
- permet de vérifier l'intégrité du message reçu ;
- Basé sur les fonctions de hachage :
  - l’émetteur calcul un condensé du message (sorte de résumé)
  - l’émetteur chiffre avec sa clé privée le condensé
  - Le récepteur décode avec la clé publique le condensé.
  - Le récepteur calcul le condensé du message reçu et le compare au condensé chiffré reçu.
- Algo de hachage : SHA-256
- Intérêt du condensé : plus rapide que de chiffrer l’intégralité du message. En effet, le chiffrement utilisé est asymétrique.

# Sécurité

**Algorithmes reconnus  sûrs**

- SHA-256, SHA-512 ou SHA-3 comme fonction de hachage ;
- HMAC utilisant SHA-256, bcrypt, scrypt ou PBKDF2 pour stocker les mots de passe;
- AES ou AES-CBC pour le chiffrement symétrique ;
- RSA-OAEP comme défini dans PKCS#1 v2.1 pour le chiffrement asymétrique ;
- enfin, pour les signatures, RSA-SSA-PSS comme spécifié dans PKCS#1 v2.1.
- Utiliser les tailles de clés suffisantes pour AES il est recommandé d'utiliser des clés de 128 bits et, pour les algorithmes basés sur RSA, des modules et exposants secrets d'au moins 2048 bits ou 3072 bits, avec des exposants publics, pour le chiffrement, supérieurs à 65536.
- Enfin **ne pas utiliser** les chiffrements DES et 3DES ou les fonctions de hachage MD5 et SHA1.

# crédits

- https://www.ssi.gouv.fr
- https://www.cnil.fr/fr
- https://openclipart.org/
- Sébastien Fourey – Ensicaen